SPP 2018.06.0 Component Release Notes

BIOS - System ROM

Top

Online ROM Flash Component for Linux - HPE ProLiant DL380 Gen9/DL360 Gen9 (P89) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-p89-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL360/DL380 Gen9 System ROM - P89

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant DL380 Gen9/DL360 Gen9 (P89) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035812.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL360/DL380 Gen9 System ROM - P89

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE Apollo 2000 Gen10/HPE ProLiant XL170r/XL190r Gen10 (U38) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-u38-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u38-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant XL170r/XL190r Gen10 System ROM - U38

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9 (U19) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u19-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9 System ROM - U19

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local

user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE Apollo 4510 Gen10/HPE ProLiant XL450 Gen10 (U40) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-u40-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u40-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant XL450 Gen10 System ROM - U40

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE ProLiant BL460c Gen10 (I41) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-i41-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-i41-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant BL460c Gen10 System ROM - I41

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Added support for the HPE D2220sb Storage Blade.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Added support for the HPE D2220sb Storage Blade.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE ProLiant BL460c Gen9/WS460c Gen9 (I36) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-i36-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant BL460c Gen9/WS460c Gen9 System ROM - I36

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant BL660c Gen9 (I38) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-i38-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned

to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant BL660c Gen9 System ROM - I38

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with

microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant DL120 Gen9 (P86) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-p86-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL120 Gen9 System ROM - P86

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant DL160 Gen9/DL180 Gen9 (U20) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u20-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL160/DL180 Gen9 System ROM - U20

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check

Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant DL20 Gen9 (U22) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u22-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory

reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL20 Gen9 System ROM - U22

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory

reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Online ROM Flash Component for Linux - HPE ProLiant DL360 Gen10 (U32) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-u32-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u32-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant DL360 Gen10 System ROM - U32

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set

to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or

the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE ProLiant DL380 Gen10 (U30) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-u30-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u30-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant DL380 Gen10 System ROM - U30

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-15-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where a system configured for HPE Scalable Persistent Memory may not properly log a backup failure event to the Integrated Management Log (IML).

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual

SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Addressed an issue where systems configured for Scalable Persistent Memory may not function properly after changing certain BIOS/Platform Configuration (RBSU) Settings such as Intel TXT support. Previously these configuration changes could have led to a loss of persistent data.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where a system configured for HPE Scalable Persistent Memory may not properly log a backup failure event to the Integrated Management Log (IML).

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Addressed an issue where systems configured for Scalable Persistent Memory may not function properly after changing certain BIOS/Platform Configuration (RBSU) Settings such as Intel TXT support. Previously these configuration changes could have led to a loss of persistent data.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE ProLiant DL385 Gen10 (A40) Servers
Version: 1.30_06-07-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-a40-1.30_2018_06_07-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-a40-1.30_2018_06_07-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant DL385 Gen10 System ROM - A40

Release Version:

1.30_06-07-2018

Last Recommended or Critical Revision:

1.30_06-07-2018

Previous Revision:

1.22_04-16-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems with 1 TB or more of memory installed may have memory resources assigned incorrectly resulting in a kernel panic or an IOMMU reported error.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems with 1 TB or more of memory installed may have memory resources assigned incorrectly resulting in a kernel panic or an IOMMU reported error.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE ProLiant DL560 Gen10/DL580 Gen10 (U34) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-u34-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u34-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant DL560/DL580 Gen10 System ROM - U34

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Added a new Power Supply Redundancy Message to inform a user of running a system configured with four power supplies in an invalid Power Supply Redundancy Mode such as 1+1 Redundancy Mode.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log

(IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Added a new Power Supply Redundancy Message to inform a user of running a system configured with four power supplies in an invalid Power Supply Redundancy Mode such as 1+1 Redundancy Mode.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE ProLiant DL560 Gen9 (P85) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-p85-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL560 Gen9 System ROM - P85

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted

processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant DL580 Gen9 (U17) Servers
Version: 2.60_05-23-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u17-2.60_2018_05_23-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL580 Gen9 System ROM - U17

Release Version:

2.60_05-23-2018

Last Recommended or Critical Revision:

2.60_05-23-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory

reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant DL60 Gen9/DL80 Gen9 (U15) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u15-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL60/DL80 Gen9 System ROM - U15

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local

user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant EC200a (U26) Server/HPE ProLiant Thin Micro TM200 (U26) Server
Version: 2.56_01-22-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u26-2.56_2018_01_22-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for Variant 2 of the Side Channel Analysis vulnerability, also known as Spectre. The revision of the microcode included in this System ROM does NOT have issues with more frequent reboots and unpredictable system behavior which impacted the previous Intel microcode which was part of the Spectre Variant 2 mitigation. Additional information is available from Intel's Security Exploit Newsroom, https://newsroom.intel.com/press-kits/security-exploits-intel-products/.

Deliverable Name:

HPE ProLiant Thin Micro TM200 Server Gen9 System ROM - U26

Release Version:

2.56_01-22-2018

Last Recommended or Critical Revision:

2.56_01-22-2018

Previous Revision:

2.52_10-25-2017

Firmware Dependencies:

None

Enhancements/New Features:

None

Problems Fixed:

Updated the Intel processor microcode to the latest version.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for Variant 2 of the Side Channel Analysis vulnerability, also known as Spectre. The revision of the microcode included in this System ROM does NOT have issues with more frequent reboots and unpredictable system behavior which impacted the previous Intel microcode which was part of the Spectre Variant 2 mitigation. Additional information is available from Intel's Security Exploit Newsroom, https://newsroom.intel.com/press-kits/security-exploits-intel-products/.

Firmware Dependencies:

None

Problems Fixed:

Updated the Intel processor microcode to the latest version.

Known Issues:

None

Enhancements

None

Online ROM Flash Component for Linux - HPE ProLiant ML110 Gen10 (U33) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-u33-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u33-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant ML110 Gen10 System ROM - U33

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE ProLiant ML110 Gen9 (P99) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-p99-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML110 Gen9 System ROM - P99

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant ML150 Gen9 (P95) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-p95-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML150 Gen9 System ROM - P95

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant ML30 Gen9 (U23) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u23-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers

and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML30 Gen9 System ROM - U23

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read

(also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant ML350 Gen10 (U41) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-u41-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u41-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant ML350 Gen10 System ROM - U41

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller

interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE ProLiant ML350 Gen9 (P92) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-p92-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML350 Gen9 System ROM - P92

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant XL170r/XL190r Gen9 (U14) Servers
Version: 2.60_05-22-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u14-2.60_2018_05_22-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with

microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL170r/190r Gen9 System ROM - U14

Release Version:

2.60_05-22-2018

Last Recommended or Critical Revision:

2.60_05-22-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant XL230a/XL250a Gen9 (U13) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u13-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL230a/XL250a Gen9 System ROM - U13

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant XL230k Gen10 (U37) Server
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-u37-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u37-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant XL230k Gen10 System ROM - U37

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.38_03-20-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Updated the integrated Intel Omni Path UEFI Driver to version 1.6.0.0.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual

SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Updated the integrated Intel Omni Path UEFI Driver to version 1.6.0.0.

Online ROM Flash Component for Linux - HPE ProLiant XL260a Gen9/XL2x260w (U24) Server
Version: 1.60_01-22-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u24-1.60_2018_01_22-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for Variant 2 of the Side Channel Analysis vulnerability, also known as Spectre. The revision of the microcode included in this System ROM does NOT have issues with more frequent reboots and unpredictable system behavior which impacted the previous Intel microcode which was part of the Spectre Variant 2 mitigation. Additional information is available from Intel's Security Exploit Newsroom, https://newsroom.intel.com/press-kits/security-exploits-intel-products/.

Deliverable Name:

HPE ProLiant XL260a Gen9/XL2x260w System ROM - U24

Release Version:

1.60_01-22-2018

Last Recommended or Critical Revision:

1.60_01-22-2018

Previous Revision:

1.50_09-25-2017

Firmware Dependencies:

None

Enhancements/New Features:

None

Problems Fixed:

Updated the Intel processor microcode to the latest version.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for Variant 2 of the Side Channel Analysis vulnerability, also known as Spectre. The revision of the microcode included in this System ROM does NOT have issues with more frequent reboots and unpredictable system behavior which impacted the previous Intel microcode which was part of the Spectre Variant 2 mitigation. Additional information is available from Intel's Security Exploit Newsroom, https://newsroom.intel.com/press-kits/security-exploits-intel-products/.

Firmware Dependencies:

None

Problems Fixed:

Updated the Intel processor microcode to the latest version.

Known Issues:

None

Online ROM Flash Component for Linux - HPE ProLiant XL270d (U25) Accelerator Tray
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u25-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL270d Accelerator Tray System ROM - U25

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant XL270d Gen10 (U45) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-u45-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u45-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant XL270d Gen10 System ROM - U45

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_04-12-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE ProLiant XL450 Gen9 (U21) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u21-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL450 Gen9 System ROM - U21

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE ProLiant XL730f/XL740f/XL750f Gen9 (U18) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-u18-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL730f/XL740f/XL750f Gen9 System ROM - U18

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE Synergy 480 Gen10 (I42) Compute Module
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-i42-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-i42-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

Deliverable Name:

HPE Synergy 480 Gen10 Compute Module System ROM - I42

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE Synergy 480 Gen9 (I37) Compute Module
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-i37-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Synergy 480 Gen9 System ROM - I37

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE Synergy 620/680 Gen9 (I40) Compute Module
Version: 2.60_05-23-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-i40-2.60_2018_05_23-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Synergy 620 Gen9 / 680 Gen9 System ROM - I40

Release Version:

2.60_05-23-2018

Last Recommended or Critical Revision:

2.60_05-23-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers

and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Linux - HPE Synergy 660 Gen10 (I43) Compute Module
Version: 1.40_06-15-2018 **(Recommended)**
Filename: RPMS/x86_64/firmware-system-i43-1.40_2018_06_15-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-i43-1.40_2018_06_15-1.1.x86_64.rpm

Important Note!

Important Notes:

Deliverable Name:

HPE Synergy 660 Gen10 Compute Module System ROM - I43

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Linux - HPE Synergy 660 Gen9 (I39) Compute Module
Version: 2.60_05-21-2018 **(Critical)**
Filename: RPMS/i386/firmware-system-i39-2.60_2018_05_21-1.1.i386.rpm

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Synergy 660 Gen9 System ROM - I39

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted

processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9 (U19) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035946.compsig; CP035946.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9 System ROM - U19

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory

reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.1, ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.1 is 5.0.3.9.
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.
The minimum CRU version for 6.7 is 6.7.10.
Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant BL460c Gen9/WS460c Gen9 (I36) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035849.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant BL460c Gen9/WS460c Gen9 System ROM - I36

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.1, ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.1 is 5.0.3.9.
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.
The minimum CRU version for 6.7 is 6.7.10.
Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant BL660c Gen9 (I38) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035823.compsig; CP035823.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant BL660c Gen9 System ROM - I38

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.1, ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.1 is 5.0.3.9.
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.
The minimum CRU version for 6.7 is 6.7.10.
Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are

also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant DL120 Gen9 (P86) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035874.compsig; CP035874.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL120 Gen9 System ROM - P86

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.

1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.

The minimum iLO version for ESXi 5.1, 5.5 and ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.

2. The "Compaq ROM Utility Driver" (CRU) must be installed and running

The minimum CRU version for ESXi 5.1 is 5.0.3.9.

The minimum CRU version for ESXi 5.5 is 5.5.4.1.

The minimum CRU version for ESXi 6.0 is 6.0.8.

The minimum CRU version for 6.5 is 6.5.8.

The minimum CRU version for 6.7 is 6.7.10.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant DL160 Gen9/DL180 Gen9 (U20) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035857.compsig; CP035857.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL160/DL180 Gen9 System ROM - U20

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.1, ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.1 is 5.0.3.9.
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.
The minimum CRU version for 6.7 is 6.7.10.
Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant DL20 Gen9 (U22) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP036398.compsig; CP036398.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL20 Gen9 System ROM - U22

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.

The minimum CRU version for 6.7 is 6.7.10.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, and 5.5 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Online ROM Flash Component for VMware - HPE ProLiant DL380 Gen9/DL360 Gen9 (P89) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035814.compsig; CP035814.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL360/DL380 Gen9 System ROM - P89

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.

1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.

The minimum iLO version for ESXi 5.1, 5.5 and ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.

2. The "Compaq ROM Utility Driver" (CRU) must be installed and running

The minimum CRU version for ESXi 5.1 is 5.0.3.9.

The minimum CRU version for ESXi 5.5 is 5.5.4.1.

The minimum CRU version for ESXi 6.0 is 6.0.8.

The minimum CRU version for 6.5 is 6.5.8.

The minimum CRU version for 6.7 is 6.7.10.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant DL560 Gen9 (P85) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035899.compsig; CP035899.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL560 Gen9 System ROM - P85

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.1, ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.1 is 5.0.3.9.
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.
The minimum CRU version for 6.7 is 6.7.10.
Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory

reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant DL580 Gen9 (U17) Servers
Version: 2.60_05-23-2018 **(Critical)**
Filename: CP035892.compsig; CP035892.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL360/DL380 Gen9 System ROM - P89

Release Version:

2.60_05-23-2018

Last Recommended or Critical Revision:

2.60_05-23-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.

1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.

The minimum iLO version for ESXi 5.5 and ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.

2. The "Compaq ROM Utility Driver" (CRU) must be installed and running

The minimum CRU version for ESXi 5.5 is 5.5.4.1.

The minimum CRU version for ESXi 6.0 is 6.0.8.

The minimum CRU version for 6.5 is 6.5.8.

The minimum CRU version for 6.7 is 6.7.10.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant DL60 Gen9/DL80 Gen9 (U15) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035902.compsig; CP035902.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL60/DL80 Gen9 System ROM - U15

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode

only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.

1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.

The minimum iLO version for ESXi 5.1, 5.5 and ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.

2. The "Compaq ROM Utility Driver" (CRU) must be installed and running

The minimum CRU version for ESXi 5.1 is 5.0.3.9.

The minimum CRU version for ESXi 5.5 is 5.5.4.1.

The minimum CRU version for ESXi 6.0 is 6.0.8.

The minimum CRU version for 6.5 is 6.5.8.

The minimum CRU version for 6.7 is 6.7.10.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted

processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant EC200a (U26) Server/HPE ProLiant Thin Micro TM200 (U26) Server
Version: 2.56_01-22-2018 (B) **(Critical)**
Filename: CP035387.compsig; CP035387.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for Variant 2 of the Side Channel Analysis vulnerability, also known as Spectre. The revision of the microcode included in this System ROM does NOT have issues with more frequent reboots and unpredictable system behavior which impacted the previous Intel microcode which was part of the Spectre Variant 2 mitigation. Additional information is available from Intel's Security Exploit Newsroom, https://newsroom.intel.com/press-kits/security-exploits-intel-products/.

Ver. 2.56_01-22-2018 (B) contains support for VMware vSphere 6.7. It is functionally equivalent to ver. 2.56_01-22-2018. It is not necessary to upgrade with version 2.56_01-22-2018 (B) if a previous component revision was used to upgrade the firmware to ver. 2.56_01-22-2018.

Deliverable Name:

HPE ProLiant Thin Micro TM200 Server Gen9 System ROM - U26

Release Version:

2.56_01-22-2018

Last Recommended or Critical Revision:

2.56_01-22-2018

Previous Revision:

2.52_10-25-2017

Firmware Dependencies:

None

Enhancements/New Features:

None

Problems Fixed:

Updated the Intel processor microcode to the latest version.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.

1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.

The minimum iLO version for ESXi 5.5 and ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.

2. The "Compaq ROM Utility Driver" (CRU) must be installed and running

The minimum CRU version for ESXi 5.5 is 5.5.4.1.

The minimum CRU version for ESXi 6.0 is 6.0.8.

The minimum CRU version for 6.5 is 6.5.8.

The minimum CRU version for 6.7 is 6.7.10.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for Variant 2 of the Side Channel Analysis vulnerability, also known as Spectre. The revision of the microcode included in this System ROM does NOT have issues with more frequent reboots and unpredictable system behavior which impacted the previous Intel microcode which was part of the Spectre Variant 2 mitigation. Additional information is available from Intel's Security Exploit Newsroom, https://newsroom.intel.com/press-kits/security-exploits-intel-products/.

Ver. 2.56_01-22-2018 (B) contains support for VMware vSphere 6.7. It is functionally equivalent to ver. 2.56_01-22-2018. It is not necessary to upgrade with version 2.56_01-22-2018 (B) if a previous component revision was used to upgrade the firmware to ver. 2.56_01-22-2018.

Firmware Dependencies:

None

Problems Fixed:

Updated the Intel processor microcode to the latest version.

Known Issues:

None

Enhancements

None

Online ROM Flash Component for VMware - HPE ProLiant ML110 Gen9 (P99) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035851.compsig; CP035851.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML110 Gen9 System ROM - P99

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.1, ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.1 is 5.0.3.9.
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.
The minimum CRU version for 6.7 is 6.7.10.
Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory

reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant ML150 Gen9 (P95) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035878.compsig; CP035878.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML150 Gen9 System ROM - P95

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates,

provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.1, ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.1 is 5.0.3.9.
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.
The minimum CRU version for 6.7 is 6.7.10.
Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant ML30 Gen9 (U23) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035706.compsig; CP035706.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML30 Gen9 System ROM - U23

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.

The minimum CRU version for 6.7 is 6.7.10.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, and 5.5 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant ML350 Gen9 (P92) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035961.compsig; CP035961.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted

processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML350 Gen9 System ROM - P92

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.1, ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.1 is 5.0.3.9.
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.
The minimum CRU version for 6.7 is 6.7.10.
Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates,

provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant XL170r/XL190r Gen9 (U14) Servers
Version: 2.60_05-22-2018 **(Critical)**
Filename: CP035888.compsig; CP035888.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL170r/190r Gen9 System ROM - U14

Release Version:

2.60_05-22-2018

Last Recommended or Critical Revision:

2.60_05-22-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.

1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.

The minimum iLO version for ESXi 5.1, 5.5 and ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.

2. The "Compaq ROM Utility Driver" (CRU) must be installed and running

The minimum CRU version for ESXi 5.1 is 5.0.3.9.

The minimum CRU version for ESXi 5.5 is 5.5.4.1.

The minimum CRU version for ESXi 6.0 is 6.0.8.

The minimum CRU version for 6.5 is 6.5.8.

The minimum CRU version for 6.7 is 6.7.10.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers

and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE ProLiant XL450 Gen9 (U21) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035821.compsig; CP035821.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL450 Gen9 System ROM - U21

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.1, ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.1 is 5.0.3.9.
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.
The minimum CRU version for 6.7 is 6.7.10.
Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with

microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE Synergy 480 Gen9 (I37) Compute Module
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035855.compsig; CP035855.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Synergy 480 Gen9 System ROM - I37

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.

The minimum CRU version for 6.7 is 6.7.10.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, and 5.5 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE Synergy 620/680 Gen9 (I40) Compute Module
Version: 2.60_05-23-2018 **(Critical)**
Filename: CP036456.compsig; CP036456.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Synergy 620 Gen9 / 680 Gen9 System ROM - I40

Release Version:

2.60_05-23-2018

Last Recommended or Critical Revision:

2.60_05-23-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.

The minimum CRU version for 6.7 is 6.7.10.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, and 5.5 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware - HPE Synergy 660 Gen9 (I39) Compute Module
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035828.compsig; CP035828.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Synergy 660 Gen9 System ROM - I39

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.

The minimum CRU version for 6.7 is 6.7.10.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, and 5.5 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for VMware ESXi- HPE ProLiant XL230a/XL250a Gen9 (U13) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: CP035826.compsig; CP035826.zip

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL230a/XL250a Gen9 System ROM - U13

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.
1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.
The minimum iLO version for ESXi 5.1, ESXi 5.5, ESXi 6.0 and ESXi 6.5 is 1.4. The minimum iLO version for ESXi 6.7 is 10.1.0.
2. The "Compaq ROM Utility Driver" (CRU) must be installed and running
The minimum CRU version for 5.1 is 5.0.3.9.
The minimum CRU version for 5.5 is 5.5.4.1.
The minimum CRU version for 6.0 is 6.0.8.
The minimum CRU version for 6.5 is 6.5.8.
The minimum CRU version for 6.7 is 6.7.10.
Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.7, 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of

system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE Apollo 2000 Gen10/HPE ProLiant XL170r/XL190r Gen10 (U38) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: cp034607.compsig; cp034607.exe

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant XL170r/XL190r Gen10 System ROM - U38

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new

optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O

Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Windows x64 - HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9 (U19) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035944.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9 System ROM - U19

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode

only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE Apollo 4510 Gen10/HPE ProLiant XL450 Gen10 (U40) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: cp034585.compsig; cp034585.exe

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant XL450 Gen10 System ROM - U40

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Windows x64 - HPE ProLiant BL460c Gen10 (I41) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: cp034627.compsig; cp034627.exe

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant BL460c Gen10 System ROM - I41

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Added support for the HPE D2220sb Storage Blade.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Added support for the HPE D2220sb Storage Blade.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Windows x64 - HPE ProLiant BL460c Gen9/WS460c Gen9 (I36) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035846.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned

to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant BL460c Gen9/WS460c Gen9 System ROM - I36

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with

microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant BL660c Gen9 (I38) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035824.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant BL660c Gen9 System ROM - I38

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant DL120 Gen9 (P86) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035875.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL120 Gen9 System ROM - P86

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check

Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant DL160 Gen9/DL180 Gen9 (U20) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035854.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local

user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL160/DL180 Gen9 System ROM - U20

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers

and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant DL20 Gen9 (U22) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp036396.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL20 Gen9 System ROM - U22

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Online ROM Flash Component for Windows x64 - HPE ProLiant DL360 Gen10 (U32) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: cp034630.compsig; cp034630.exe

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant DL360 Gen10 System ROM - U32

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Windows x64 - HPE ProLiant DL380 Gen10 (U30) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: cp034618.compsig; cp034618.exe

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant DL380 Gen10 System ROM - U30

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-15-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where a system configured for HPE Scalable Persistent Memory may not properly log a backup failure event to the Integrated Management Log (IML).

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Addressed an issue where systems configured for Scalable Persistent Memory may not function properly after changing certain BIOS/Platform Configuration (RBSU) Settings such as Intel TXT support. Previously these configuration changes could have led to a loss of persistent data.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where a system configured for HPE Scalable Persistent Memory may not properly log a backup failure event to the Integrated Management Log (IML).

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Addressed an issue where systems configured for Scalable Persistent Memory may not function properly after changing certain BIOS/Platform Configuration (RBSU) Settings such as Intel TXT support. Previously these configuration changes could have led to a loss of persistent data.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Windows x64 - HPE ProLiant DL385 Gen10 (A40) Servers
Version: 1.30_06-07-2018 **(Recommended)**
Filename: cp035120.compsig; cp035120.exe

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant DL385 Gen10 System ROM - A40

Release Version:

1.30_06-07-2018

Last Recommended or Critical Revision:

1.30_06-07-2018

Previous Revision:

1.22_04-16-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems with 1 TB or more of memory installed may have memory resources assigned incorrectly resulting in a kernel panic or an IOMMU reported error.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems with 1 TB or more of memory installed may have memory resources assigned incorrectly resulting in a kernel panic or an IOMMU reported error.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of

the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Windows x64 - HPE ProLiant DL560 Gen10/DL580 Gen10 (U34) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: cp034629.compsig; cp034629.exe

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant DL560/DL580 Gen10 System ROM - U34

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when

launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Added a new Power Supply Redundancy Message to inform a user of running a system configured with four power supplies in an invalid Power Supply Redundancy Mode such as 1+1 Redundancy Mode.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Added a new Power Supply Redundancy Message to inform a user of running a system configured with four power supplies in an invalid Power Supply Redundancy Mode such as 1+1 Redundancy Mode.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Windows x64 - HPE ProLiant DL560 Gen9 (P85) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035897.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL560 Gen9 System ROM - P85

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with

microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant DL580 Gen9 (U17) Servers
Version: 2.60_05-23-2018 **(Critical)**
Filename: cp035893.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL360/DL380 Gen9 System ROM - P89

Release Version:

2.60_05-23-2018

Last Recommended or Critical Revision:

2.60_05-23-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local

user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant DL60 Gen9/DL80 Gen9 (U15) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035903.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant DL60/DL80 Gen9 System ROM - U15

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated

Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant EC200a (U26) Server/HPE ProLiant Thin Micro TM200 (U26) Server
Version: 2.56_01-22-2018 (B) **(Critical)**
Filename: cp034916.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for Variant 2 of the Side Channel Analysis vulnerability, also known as Spectre. The revision of the microcode included in this System ROM does NOT have issues with more frequent reboots and unpredictable system behavior which impacted the previous Intel microcode which was part of the Spectre Variant 2 mitigation. Additional information is available from Intel's Security Exploit Newsroom, https://newsroom.intel.com/press-kits/security-exploits-intel-products/.

Deliverable Name:

HPE ProLiant Thin Micro TM200 Server Gen9 System ROM - U26

Release Version:

2.56_01-22-2018

Last Recommended or Critical Revision:

2.56_01-22-2018

Previous Revision:

2.52_10-25-2017

Firmware Dependencies:

None

Enhancements/New Features:

None

Problems Fixed:

Updated the Intel processor microcode to the latest version.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for Variant 2 of the Side Channel Analysis vulnerability, also known as Spectre. The revision of the microcode included in this System ROM does NOT have issues with more frequent reboots and unpredictable system behavior which impacted the previous Intel microcode which was part of the Spectre Variant 2 mitigation. Additional information is available from Intel's Security Exploit Newsroom, https://newsroom.intel.com/press-kits/security-exploits-intel-products/.

Firmware Dependencies:

None

Problems Fixed:

Updated the Intel processor microcode to the latest version.

Known Issues:

None

Online ROM Flash Component for Windows x64 - HPE ProLiant ML110 Gen10 (U33) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: cp034613.compsig; cp034613.exe

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant ML110 Gen10 System ROM - U33

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact

systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Windows x64 - HPE ProLiant ML110 Gen9 (P99) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035847.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML110 Gen9 System ROM - P99

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant ML150 Gen9 (P95) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035876.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML150 Gen9 System ROM - P95

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with

microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant ML30 Gen9 (U23) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035704.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML30 Gen9 System ROM - U23

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant ML350 Gen10 (U41) Servers
Version: 1.40_06-15-2018 **(Recommended)**
Filename: cp034641.compsig; cp034641.exe

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant ML350 Gen10 System ROM - U41

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Windows x64 - HPE ProLiant ML350 Gen9 (P92) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035797.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant ML350 Gen9 System ROM - P92

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant XL170r/XL190r Gen9 (U14) Servers
Version: 2.60_05-22-2018 **(Critical)**
Filename: cp035890.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL170r/190r Gen9 System ROM - U14

Release Version:

2.60_05-22-2018

Last Recommended or Critical Revision:

2.60_05-22-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted

processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant XL230a/XL250a Gen9 (U13) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035811.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL230a/XL250a Gen9 System ROM - U13

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant XL230k Gen10 (U37) Server
Version: 1.40_06-15-2018 **(Recommended)**
Filename: cp034595.compsig; cp034595.exe

Important Note!

Important Notes:

None

Deliverable Name:

HPE ProLiant XL230k Gen10 System ROM - U37

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.38_03-20-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Updated the integrated Intel Omni Path UEFI Driver to version 1.6.0.0.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

None

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Updated the integrated Intel Omni Path UEFI Driver to version 1.6.0.0.

Online ROM Flash Component for Windows x64 - HPE ProLiant XL270d (U25) Accelerator Tray
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035818.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL270d Accelerator Tray System ROM - U25

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE ProLiant XL450 Gen9 (U21) Servers
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035810.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE ProLiant XL450 Gen9 System ROM - U21

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated

Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE Synergy 480 Gen10 (I42) Compute Module
Version: 1.40_06-15-2018 **(Recommended)**
Filename: cp034563.compsig; cp034563.exe

Important Note!

Important Notes:

Deliverable Name:

HPE Synergy 480 Gen10 Compute Module System ROM - I42

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Windows x64 - HPE Synergy 480 Gen9 (I37) Compute Module
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035852.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Synergy 480 Gen9 System ROM - I37

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local

user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Online ROM Flash Component for Windows x64 - HPE Synergy 620/680 Gen9 (I40) Compute Module
Version: 2.60_05-23-2018 **(Critical)**
Filename: cp036454.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Synergy 620 Gen9 / 680 Gen9 System ROM - I40

Release Version:

2.60_05-23-2018

Last Recommended or Critical Revision:

2.60_05-23-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned

to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Filename: cp034565.compsig; cp034565.exe

Important Note!

Important Notes:

Deliverable Name:

HPE Synergy 660 Gen10 Compute Module System ROM - I43

Release Version:

1.40_06-15-2018

Last Recommended or Critical Revision:

1.40_06-15-2018

Previous Revision:

1.36_02-14-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

Firmware Dependencies:

None

Problems Fixed:

Addressed an issue where systems may experience an 389-Unexpected Shutdown and Restart, logged in the iLO Integrated Management Log (IML). This issue is not unique to HPE servers.

Addressed an issue where the Embedded Diagnostics may not launch properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Integrated Management Log (IML) Viewer in the System Utilities menu may become unresponsive when launched.

Addressed an issue where the HPE Dual SD Card USB Module may not boot properly when the UEFI POST Discovery Mode option is set to Force Fast Discovery.

Addressed an issue where the Trusted Platform Module (TPM) Firmware update may not complete properly when the TPM is configured for TPM 2.0 Mode. This issue does not impact systems configured with a TPM operating in TPM 1.2 mode.

Addressed an issue where the system may not be able to boot to Intelligent Provisioning when a third party USB Key was installed in one of the server USB Ports. This issue was seen with a specific USB Key and has not been seen with other devices.

Addressed an issue where Integrated Lights-Out (iLO) Virtual Media may not boot properly when the UEFI POST Discovery Mode option is set to Force Full Discovery.

Addressed an issue where the system may become unresponsive during POST or experience a Red Screen on the next boot following an I/O Machine Check Failure at runtime.

Addressed an issue where a system configured with the internal SD Card disabled from BIOS/Platform Configuration (RBSU) and an HPE Dual SD card installed would not boot from the HPE Dual SD card USB Module when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where a system configured with an optional HPE CN1200E-T adapter would not boot properly when configured in Legacy Boot Mode. This issue does not impact systems configured in UEFI Boot Mode.

Addressed an issue where systems configured with HPE s100i Software RAID may experience a failed RAID volume on a system reset.

Known Issues:

None

Enhancements

Added support for the latest VMware vSphere Secure Boot Certificate.

Added support to decode certain Machine Check Exceptions to a specific failing PCIe device. Previous versions of the System ROM would log a generic Machine Check event to the Integrated Management Log (IML) for these error events.

Added a new BIOS/Platform Configuration (RBSU) Memory Controller Interleaving menu. This option allows disabling memory controller interleaving which may improve memory performance for systems configured with an unbalanced memory configuration.

Added a new BIOS/Platform Configuration (RBSU) Processor Jitter Control Optimization menu for Jitter Smoothing Support. This new optimization setting allows customers to choose between optimizing Auto-tuned mode for maximum throughput performance, low latency, or the default - zero latency.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Updated the language translations (non-English modes) for System Utilities.

Online ROM Flash Component for Windows x64 - HPE Synergy 660 Gen9 (I39) Compute Module
Version: 2.60_05-21-2018 **(Critical)**
Filename: cp035829.exe

Important Note!

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read

(also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Deliverable Name:

HPE Synergy 660 Gen9 System ROM - I39

Release Version:

2.60_05-21-2018

Last Recommended or Critical Revision:

2.60_05-21-2018

Previous Revision:

2.56_01-22-2018

Firmware Dependencies:

None

Enhancements/New Features:

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Fixes

Important Notes:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Firmware Dependencies:

None

Problems Fixed:

This revision of the System ROM includes the latest revision of the Intel microcode which, in combination with operating system updates, provides mitigation for the Speculative Store Bypass (also known as Variant 4) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3639. Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

This revision of the System ROM includes the latest revision of the Intel microcode which provides mitigation for the Rogue Register Read (also known as Variant 3a) security vulnerability. A Medium level CVE has been assigned to this issue with ID CVE-2018-3640. Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis. This security vulnerability is not unique to HPE servers and impacts any systems utilizing impacted processors.

Addressed an issue where uncorrectable Quick Path Interlink (QPI) errors would not be reported properly and logged to the Integrated Management Log. Previously, the system would become unresponsive during boot with no indication of a failure.

Addressed an issue where systems configured Intel Xeon E5-2600 v4 processors and 64GB LRDIMMs may experience a Machine Check Exception or NMI event when under heavy stress. This issue is not unique to HPE Servers.

Addressed an issue where the HPE RESTful settings for Software Initiator iSCSI may not be available in the resource registry.

Known Issues:

None

Enhancements

Added support to allow for the ROM Based Setup Utility (RBSU) Power Regulator setting to be set to Static Low or OS Control Mode when the Processor Power and Utilization Support was disabled. Previous ROMs required the Power Regulator to be configured for Static High Mode only.

Updated the RESTful API HPE BIOS Attribute Registry resources to match the latest BIOS/Platform Configuration options.

Driver - Chipset

Top

Identifiers for AMD EPYC Processors for Windows
Version: 1.0.0.0 (C) **(Optional)**
Filename: cp034065.compsig; cp034065.exe

Enhancements

- Added support for the HPE ProLiant DL325 Gen10.
- Corrected copyright string on version control DLL.

Identifiers for Intel Xeon Processor Scalable Family for Windows Server 2012 R2 and Server 2016
Version: 10.1.2.86 (B) **(Optional)**
Filename: cp034634.compsig; cp034634.exe

Fixes

Corrected a potential installation failure that could occur when Windows Device Guard is enabled.

Enhancements

Added support for the HPE ProLiant XL420 Gen10.

Driver - Network

Top

HPE Broadcom NetXtreme-E Driver for Windows Server 2012 R2
Version: 212.0.89.0 **(Optional)**
Filename: cp034199.compsig; cp034199.exe

Important Note!

HPE recommends the firmware provided in *HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a link flip when connected to an Arista-series switch.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E Driver for Windows Server 2016
Version: 212.0.89.0 **(Optional)**
Filename: cp034200.compsig; cp034200.exe

Important Note!

HPE recommends the firmware provided in *HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a link flip when connected to an Arista-series switch.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6
Version: 1.9.1-212.0.99.0 **(Optional)**
Filename: kmod-bnxt_en-1.9.1-212.0.99.0.rhel6u9.x86_64.compsig; kmod-bnxt_en-1.9.1-212.0.99.0.rhel6u9.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Linux x86_64*, version 1.3.10 or later, for use with these drivers.

Fixes

This product corrects a firmware package version issue seen when using ethtool -i.
This product corrects a firmware timeout error seen when a VF link changes.
This product corrects a VF PCIE link speed/width detection error.
This product corrects a SmartNIC PCI VF ID error.
This product corrects a system hang seen during a reboot on a SmartNIC.
This product addresses a system crash seen when using ethtool.
This product corrects an issue where the "ip link show" command displays incorrect VF MAC addresses on a PF.
This product corrects a VF range checking error seen when using iproute2 VF commands.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 7
Version: 1.9.1-212.0.99.0 **(Optional)**
Filename: kmod-bnxt_en-1.9.1-212.0.99.0.rhel7u4.x86_64.compsig; kmod-bnxt_en-1.9.1-212.0.99.0.rhel7u4.x86_64.rpm; kmod-bnxt_en-1.9.1-212.0.99.0.rhel7u5.x86_64.compsig; kmod-bnxt_en-1.9.1-212.0.99.0.rhel7u5.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Linux x86_64*, version 1.3.10 or later, for use with these drivers.

Fixes

This product corrects a firmware package version issue seen when using ethtool -i.

This product corrects a firmware timeout error seen when a VF link changes.
This product corrects a VF PCIE link speed/width detection error.
This product corrects a SmartNIC PCI VF ID error.
This product corrects a system hang seen during a reboot on a SmartNIC.
This product addresses a system crash seen when using ethtool.
This product corrects an issue where the "ip link show" command displays incorrect VF MAC addresses on a PF.
This product corrects a VF range checking error seen when using iproute2 VF commands.

Enhancements

This product now supports Red Hat Enterprise Linux 7.5.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E Drivers for SUSE Linux Enterprise Server 11 x86_64
Version: 1.9.1-212.0.99.0 **(Optional)**
Filename: bnxt_en-kmp-default-1.9.1_3.0.101_63-212.0.99.0.sles11sp4.x86_64.compsig; bnxt_en-kmp-default-1.9.1_3.0.101_63-212.0.99.0.sles11sp4.x86_64.rpm; bnxt_en-kmp-xen-1.9.1_3.0.101_63-212.0.99.0.sles11sp4.x86_64.compsig; bnxt_en-kmp-xen-1.9.1_3.0.101_63-212.0.99.0.sles11sp4.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Linux x86_64*, version 1.3.10 or later, for use with these drivers.

Fixes

This product corrects a firmware package version issue seen when using ethtool -i.
This product corrects a firmware timeout error seen when a VF link changes.
This product corrects a VF PCIE link speed/width detection error.
This product corrects a SmartNIC PCI VF ID error.
This product corrects a system hang seen during a reboot on a SmartNIC.
This product addresses a system crash seen when using ethtool.
This product corrects an issue where the "ip link show" command displays incorrect VF MAC addresses on a PF.
This product corrects a VF range checking error seen when using iproute2 VF commands.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E Drivers for SUSE Linux Enterprise Server 12 x86_64
Version: 1.9.1-212.0.99.0 **(Optional)**
Filename: bnxt_en-kmp-default-1.9.1_k4.4.21_69-212.0.99.0.sles12sp2.x86_64.compsig; bnxt_en-kmp-default-1.9.1_k4.4.21_69-212.0.99.0.sles12sp2.x86_64.rpm; bnxt_en-kmp-default-1.9.1_k4.4.73_5-212.0.99.0.sles12sp3.x86_64.compsig; bnxt_en-kmp-default-1.9.1_k4.4.73_5-212.0.99.0.sles12sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Linux x86_64*, version 1.3.10 or later, for use with these drivers.

Fixes

This product corrects a firmware package version issue seen when using ethtool -i.
This product corrects a firmware timeout error seen when a VF link changes.
This product corrects a VF PCIE link speed/width detection error.
This product corrects a SmartNIC PCI VF ID error.
This product corrects a system hang seen during a reboot on a SmartNIC.
This product addresses a system crash seen when using ethtool.
This product corrects an issue where the "ip link show" command displays incorrect VF MAC addresses on a PF.
This product corrects a VF range checking error seen when using iproute2 VF commands.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E RoCE Library for Red Hat Enterprise Linux 6 Update 9
Version: 212.0.82.0 **(Optional)**
Filename: libbnxtre-212.0.82.0-rhel6u9.x86_64.compsig; libbnxtre-212.0.82.0-rhel6u9.x86_64.rpm; README

Prerequisites

HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6, version 1.9.1-212.0.99.0 or later, must be installed before installing this product.

The libibverb package must be installed on the target system prior to the installation of the RoCE library. If not already present, the libibverb package can be obtained from the operating system installation media.

Enhancements

This library is updated to maintain compatibility with firmware version 1.3.x.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E RoCE Library for Red Hat Enterprise Linux 7 Update 4
Version: 212.0.82.0 **(Optional)**
Filename: libbnxt_re-212.0.82.0-rhel7u4.x86_64.compsig; libbnxt_re-212.0.82.0-rhel7u4.x86_64.rpm; README

Prerequisites

HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6, version 1.9.1-212.0.99.0 or later, must be installed before installing this product.

The libibverb package must be installed on the target system prior to the installation of the RoCE library. If not already present, the libibverb package can be obtained from the operating system installation media.

Enhancements

This library is updated to maintain compatibility with firmware version 1.3.x.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E RoCE Library for Red Hat Enterprise Linux 7 Update 5
Version: 212.0.82.0 **(Optional)**
Filename: libbnxt_re-212.0.82.0-rhel7u5.x86_64.compsig; libbnxt_re-212.0.82.0-rhel7u5.x86_64.rpm; README

Prerequisites

HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6, version 1.9.1-212.0.99.0 or later, must be installed before installing this product.

The libibverb package must be installed on the target system prior to the installation of the RoCE library. If not already present, the libibverb package can be obtained from the operating system installation media.

Enhancements

Initial release.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E RoCE Library for SUSE Linux Enterprise Server 11 SP4
Version: 212.0.82.0 **(Optional)**
Filename: libbnxtre-212.0.82.0-sles11sp4.x86_64.compsig; libbnxtre-212.0.82.0-sles11sp4.x86_64.rpm; README

Prerequisites

HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6, version 1.9.1-212.0.99.0 or later, must be installed before installing this product.

The libibverb package must be installed on the target system prior to the installation of the RoCE library. If not already present, the libibverb package can be obtained from the operating system installation media.

Enhancements

This library is updated to maintain compatibility with firmware version 1.3.x.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E RoCE Library for SUSE Linux Enterprise Server 12 SP2
Version: 212.0.82.0 **(Optional)**
Filename: libbnxtre-212.0.82.0-sles12sp2.x86_64.compsig; libbnxtre-212.0.82.0-sles12sp2.x86_64.rpm; README

Prerequisites

HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6, version 1.9.1-212.0.99.0 or later, must be installed before installing this product.

The libibverb package must be installed on the target system prior to the installation of the RoCE library. If not already present, the libibverb package can be obtained from the operating system installation media.

Enhancements

This library is updated to maintain compatibility with firmware version 1.3.x.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E RoCE Library for SUSE Linux Enterprise Server 12 SP3
Version: 212.0.82.0 **(Optional)**
Filename: libbnxt_re-212.0.82.0-sles12sp3.x86_64.compsig; libbnxt_re-212.0.82.0-sles12sp3.x86_64.rpm; README

Prerequisites

HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6, version 1.9.1-212.0.99.0 or later, must be installed before installing this product.

The libibverb package must be installed on the target system prior to the installation of the RoCE library. If not already present, the libibverb package can be obtained from the operating system installation media.

Enhancements

This library is updated to maintain compatibility with firmware version 1.3.x.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NX1 1Gb Driver for Windows Server x64 Editions
Version: 212.0.0.0 **(Optional)**
Filename: cp034731.compsig; cp034731.exe

Important Note!

HPE recommends the firmware provided in *HPE Broadcom NX1 Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a Windows Stop Error (0x133) when the system is operating in a heavily stressed environment.

Enhancements

The component installer for this package is now digitally signed.

Supported Devices and Features

This driver supports the following network adapters:

- HP Ethernet 1Gb 2-port 330i Adapter (22BD)
- HP Ethernet 1Gb 4-port 331i Adapter (22BE)
- HPE Ethernet 1Gb 4-port 331FLR Adapter
- HPE Ethernet 1Gb 4-port 331T Adapter
- HP Ethernet 1Gb 2-port 332i Adapter (2133)
- HP Ethernet 1Gb 2-port 332i Adapter (22E8)
- HPE Ethernet 1Gb 2-port 332T Adapter

HPE Broadcom tg3 Ethernet Drivers for Red Hat Enterprise Linux 6 x86_64
Version: 3.137w-1 **(Optional)**
Filename: kmod-tg3-3.137w-1.rhel6u8.x86_64.compsig; kmod-tg3-3.137w-1.rhel6u8.x86_64.rpm; kmod-tg3-3.137w-1.rhel6u9.x86_64.compsig; kmod-tg3-3.137w-1.rhel6u9.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE NX1 Broadcom Online Firmware Upgrade Utility for Linux x86_64,* version 2.21.3 or later, for use with these drivers.

Fixes

This product addresses a traffic stop seen when running ping flood and iperf3 tests.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 1Gb 2-port 330i Adapter (22BD)
- HP Ethernet 1Gb 4-port 331i Adapter (22BE)
- HP Ethernet 1Gb 4-port 331FLR Adapter
- HP Ethernet 1Gb 4-port 331T Adapter
- HP Ethernet 1Gb 2-port 332i Adapter (2133)
- HP Ethernet 1Gb 2-port 332i Adapter (22E8)
- HP Ethernet 1Gb 2-port 332T Adapter

HPE Broadcom tg3 Ethernet Drivers for Red Hat Enterprise Linux 7 x86_64
Version: 3.137w-1 **(Optional)**
Filename: kmod-tg3-3.137w-1.rhel7u4.x86_64.compsig; kmod-tg3-3.137w-1.rhel7u4.x86_64.rpm; kmod-tg3-3.137w-1.rhel7u5.x86_64.compsig;

kmod-tg3-3.137w-1.rhel7u5.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE NX1 Broadcom Online Firmware Upgrade Utility for Linux x86_64,* version 2.21.3 or later, for use with these drivers.

Fixes

This product addresses a traffic stop seen when running ping flood and iperf3 tests.

Enhancements

This product now supports Red Hat Enterprise Linux 7.5.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 1Gb 2-port 330i Adapter (22BD)
- HP Ethernet 1Gb 4-port 331i Adapter (22BE)
- HP Ethernet 1Gb 4-port 331FLR Adapter
- HP Ethernet 1Gb 4-port 331T Adapter
- HP Ethernet 1Gb 2-port 332i Adapter (2133)
- HP Ethernet 1Gb 2-port 332i Adapter (22E8)
- HP Ethernet 1Gb 2-port 332T Adapter

HPE Broadcom tg3 Ethernet Drivers for SUSE Linux Enterprise Server 11 x86_64
Version: 3.137w-1 **(Optional)**
Filename: README; tg3-kmp-default-3.137w_3.0.101_63-1.sles11sp4.x86_64.compsig; tg3-kmp-default-3.137w_3.0.101_63-1.sles11sp4.x86_64.rpm; tg3-kmp-default-3.137w_3.0.76_0.11-1.sles11sp3.x86_64.compsig; tg3-kmp-default-3.137w_3.0.76_0.11-1.sles11sp3.x86_64.rpm; tg3-kmp-xen-3.137w_3.0.101_63-1.sles11sp4.x86_64.compsig; tg3-kmp-xen-3.137w_3.0.101_63-1.sles11sp4.x86_64.rpm; tg3-kmp-xen-3.137w_3.0.76_0.11-1.sles11sp3.x86_64.compsig; tg3-kmp-xen-3.137w_3.0.76_0.11-1.sles11sp3.x86_64.rpm

Important Note!

HPE recommends the firmware provided in *HPE NX1 Broadcom Online Firmware Upgrade Utility for Linux x86_64,* version 2.21.3 or later, for use with these drivers.

Fixes

This product addresses a traffic stop seen when running ping flood and iperf3 tests.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 1Gb 2-port 330i Adapter (22BD)
- HP Ethernet 1Gb 4-port 331i Adapter (22BE)
- HP Ethernet 1Gb 4-port 331FLR Adapter
- HP Ethernet 1Gb 4-port 331T Adapter
- HP Ethernet 1Gb 2-port 332i Adapter (2133)
- HP Ethernet 1Gb 2-port 332i Adapter (22E8)
- HP Ethernet 1Gb 2-port 332T Adapter

HPE Broadcom tg3 Ethernet Drivers for SUSE Linux Enterprise Server 12 x86_64
Version: 3.137w-1 **(Optional)**
Filename: README; tg3-kmp-default-3.137w_k4.4.21_69-1.sles12sp2.x86_64.compsig; tg3-kmp-default-3.137w_k4.4.21_69-1.sles12sp2.x86_64.rpm; tg3-kmp-default-3.137w_k4.4.73_5-1.sles12sp3.x86_64.compsig; tg3-kmp-default-3.137w_k4.4.73_5-1.sles12sp3.x86_64.rpm

Important Note!

HPE recommends the firmware provided in *HPE NX1 Broadcom Online Firmware Upgrade Utility for Linux x86_64,* version 2.21.3 or later, for use with these drivers.

Fixes

This product addresses a traffic stop seen when running ping flood and iperf3 tests.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 1Gb 2-port 330i Adapter (22BD)
- HP Ethernet 1Gb 4-port 331i Adapter (22BE)
- HP Ethernet 1Gb 4-port 331FLR Adapter
- HP Ethernet 1Gb 4-port 331T Adapter
- HP Ethernet 1Gb 2-port 332i Adapter (2133)
- HP Ethernet 1Gb 2-port 332i Adapter (22E8)
- HP Ethernet 1Gb 2-port 332T Adapter

HPE Broadcom tg3 Ethernet Drivers for VMware vSphere 6.0
Version: 2017.07.07 **(Optional)**
Filename: cp032239.compsig; cp032239.zip
Driver Name and Version:

Important Note!

HP recommends the firmware provided in *HPE Broadcom NX1 Online Firmware Upgrade Utility for VMware*, version 1.17.15, for use with this driver.

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

Fixes

This product now correctly identifies the HP Ethernet 1Gb 2-port 332i Adapter (22E8).

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 1Gb 2-port 330i Adapter
- HP Ethernet 1Gb 4-port 331FLR Adapter
- HP Ethernet 1Gb 4-port 331i Adapter
- HP Ethernet 1Gb 4-port 331i-SPI Adapter
- HP Ethernet 1Gb 4-port 331T Adapter
- HP Ethernet 1Gb 2-port 332i Adapter (2133)
- HP Ethernet 1Gb 2-port 332i Adapter (22E8)
- HP Ethernet 1Gb 2-port 332T Adapter

HPE Emulex 10/20 GbE Driver for VMware vSphere 6.5
Version: 2018.06.04 **(Optional)**
Filename: cp034443.compsig; cp034443.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters for VMware vSphere 6.5*, version 2018.06.01 or later, for use with this driver.

Fixes

This product addresses an error handling issue seen during driver initialization.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20 GbE Driver for Windows Server 2012
Version: 12.0.1115.0 **(Optional)**

Filename: cp034398.compsig; cp034398.exe

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Windows (x64),* version 2018.06.01 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a link always staying connected when a Virtual Connect(VC) module is connected.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20 GbE Driver for Windows Server 2012 R2
Version: 12.0.1115.0 **(Optional)**
Filename: cp034399.compsig; cp034399.exe

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Windows (x64),* version 2018.06.01 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a link always staying connected when a Virtual Connect(VC) module is connected.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20 GbE Driver for Windows Server 2016
Version: 12.0.1115.0 **(Optional)**
Filename: cp034400.compsig; cp034400.exe

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Windows (x64),* version 2018.06.01 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a link always staying connected when a Virtual Connect(VC) module is connected.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20 GbE iSCSI Driver for VMware vSphere 6.0
Version: 2018.06.04 **(Optional)**
Filename: cp034440.compsig; cp034440.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters for VMware vSphere 6.0*, version 2018.06.01 or later, for use with this driver.

Fixes

This product is updated to maintain compatibility with firmware version 12.0.1086.x.

Supported Devices and Features

These drivers support the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20 GbE iSCSI Driver for Windows Server 2012
Version: 12.0.1104.0 **(Optional)**
Filename: cp034401.compsig; cp034401.exe

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Windows (x64),* version 2018.06.01 or later, for use with this driver.

Enhancements

This product is updated to maintain compatibility with firmware version 12.0.1086.x.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20 GbE iSCSI Driver for Windows Server 2012 R2
Version: 12.0.1104.0 **(Optional)**
Filename: cp034402.compsig; cp034402.exe

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Windows (x64),* version 2018.06.01 or later, for use with this driver.

Enhancements

This product is updated to maintain compatibility with firmware version 12.0.1086.x.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter

- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20 GbE iSCSI Driver for Windows Server 2016
Version: 12.0.1104.0 **(Optional)**
Filename: cp034403.compsig; cp034403.exe

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Windows (x64),* version 2018.06.01 or later, for use with this driver.

Enhancements

This product is updated to maintain compatibility with firmware version 12.0.1086.x.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20GbE Drivers for Red Hat Enterprise Linux 6 x86_64
Version: 12.0.1110.11-1 **(Optional)**
Filename: kmod-be2net-12.0.1110.11-1.rhel6u8.x86_64.compsig; kmod-be2net-12.0.1110.11-1.rhel6u8.x86_64.rpm; kmod-be2net-12.0.1110.11-1.rhel6u9.x86_64.compsig; kmod-be2net-12.0.1110.11-1.rhel6u9.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Linux (x64)*, version 2018.06.01 for use with these drivers.

Enhancements

This product is updated to maintain compatibility with firmware version 2018.06.01-1.x.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20GbE Drivers for Red Hat Enterprise Linux 7 x86_64
Version: 12.0.1110.11-1 **(Optional)**
Filename: kmod-be2net-12.0.1110.11-1.rhel7u4.x86_64.compsig; kmod-be2net-12.0.1110.11-1.rhel7u4.x86_64.rpm; kmod-be2net-12.0.1110.11-1.rhel7u5.x86_64.compsig; kmod-be2net-12.0.1110.11-1.rhel7u5.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Linux (x64)*, version 2018.06.01 for use with these drivers.

Enhancements

This product now supports Red Hat Enterprise Linux 7.5.

This product is updated to maintain compatibility with firmware version 2018.06.01-1.x.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20GbE Drivers for SUSE Linux Enterprise Server 11 x86_64
Version: 12.0.1110.11-1 **(Optional)**
Filename: be2net-kmp-default-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.compsig; be2net-kmp-default-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.rpm; be2net-kmp-default-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.compsig; be2net-kmp-default-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.rpm; be2net-kmp-xen-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.compsig; be2net-kmp-xen-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.rpm; be2net-kmp-xen-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.compsig; be2net-kmp-xen-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Linux (x64)*, version 2018.06.01 for use with these drivers.

Enhancements

This product is updated to maintain compatibility with firmware version 2018.06.01-1.x.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20GbE Drivers for SUSE Linux Enterprise Server 12 x86_64
Version: 12.0.1110.11-1 **(Optional)**
Filename: be2net-kmp-default-12.0.1110.11_k4.4.103_6.38-1.sles12sp3MU5.x86_64.compsig; be2net-kmp-default-12.0.1110.11_k4.4.103_6.38-1.sles12sp3MU5.x86_64.rpm; be2net-kmp-default-12.0.1110.11_k4.4.21_69-1.sles12sp2.x86_64.compsig; be2net-kmp-default-12.0.1110.11_k4.4.21_69-1.sles12sp2.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Linux (x64)*, version 2018.06.01 for use with these drivers.

Enhancements

This product is updated to maintain compatibility with firmware version 2018.06.01-1.x.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20GbE Drivers for VMware vSphere 6.0
Version: 2018.06.04 **(Optional)**
Filename: cp034442.compsig; cp034442.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters for VMware vSphere 6.0*, version 2018.06.01 or later, for use with this driver.

Fixes

This product addresses an error handling issue seen during driver initialization.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20GbE iSCSI Driver for VMware vSphere 6.5
Version: 2018.06.04 **(Optional)**
Filename: cp034441.compsig; cp034441.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters for VMware vSphere 6.5*, version or later, for use with this driver.

Fixes

This product is updated to maintain compatibility with firmware version 12.0.1086.x.

Supported Devices and Features

These drivers support the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20GbE iSCSI Drivers for Red Hat Enterprise Linux 6 x86_64
Version: 12.0.1110.11-1 **(Optional)**
Filename: kmod-be2iscsi-12.0.1110.11-1.rhel6u8.x86_64.compsig; kmod-be2iscsi-12.0.1110.11-1.rhel6u8.x86_64.rpm; kmod-be2iscsi-12.0.1110.11-1.rhel6u9.x86_64.compsig; kmod-be2iscsi-12.0.1110.11-1.rhel6u9.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Linux (x64)*, version 2018.06.01 for use with these drivers.

Fixes

This product corrects an installer script failure seen while uninstalling the iSCSI driver.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter

HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20GbE iSCSI Drivers for Red Hat Enterprise Linux 7 x86_64
Version: 12.0.1110.11-1 **(Optional)**
Filename: kmod-be2iscsi-12.0.1110.11-1.rhel7u4.x86_64.compsig; kmod-be2iscsi-12.0.1110.11-1.rhel7u4.x86_64.rpm; kmod-be2iscsi-12.0.1110.11-1.rhel7u5.x86_64.compsig; kmod-be2iscsi-12.0.1110.11-1.rhel7u5.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Linux (x64)*, version 2018.06.01 for use with these drivers.

Fixes

This product corrects an installer script failure seen while uninstalling the iSCSI driver.

Enhancements

This product now supports Red Hat Enterprise Linux 7.5.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20GbE iSCSI Drivers for SUSE Linux Enterprise Server 11 x86_64
Version: 12.0.1110.11-1 **(Optional)**
Filename: be2iscsi-kmp-default-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.compsig; be2iscsi-kmp-default-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.rpm; be2iscsi-kmp-default-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.compsig; be2iscsi-kmp-default-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.rpm; be2iscsi-kmp-xen-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.compsig; be2iscsi-kmp-xen-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.rpm; be2iscsi-kmp-xen-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.compsig; be2iscsi-kmp-xen-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Linux (x64)*, version 2018.06.01 for use with these drivers.

Fixes

This product corrects an installer script failure seen while uninstalling the iSCSI driver.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex 10/20GbE iSCSI Drivers for SUSE Linux Enterprise Server 12 x86_64
Version: 12.0.1110.11-1 **(Optional)**
Filename: be2iscsi-kmp-default-12.0.1110.11_k4.4.103_6.38-1.sles12sp3MU5.x86_64.compsig; be2iscsi-kmp-default-12.0.1110.11_k4.4.103_6.38-1.sles12sp3MU5.x86_64.rpm; be2iscsi-kmp-default-12.0.1110.11_k4.4.21_69-1.sles12sp2.x86_64.compsig; be2iscsi-kmp-default-12.0.1110.11_k4.4.21_69-1.sles12sp2.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Firmware Flash for Emulex Converged Network Adapters - Linux (x64)*, version 2018.06.01 for use with these drivers.

Fixes

This product corrects an installer script failure seen while uninstalling the iSCSI driver.

Supported Devices and Features

This driver supports the following network adapters:

- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Intel E1R Driver for Windows Server 2012
Version: 12.14.8.0 **(Optional)**
Filename: cp028837.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.0.0.25 or later, for use with this driver.

Fixes

This driver addresses an issue that results in the failure of a Powershell command that contains an adapter name.

Supported Devices and Features

This driver supports the following HPE Intel E1R network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361FLB Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366i Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter
- HP Ethernet 1Gb 2-port 367i Adapter

HPE Intel E1R Driver for Windows Server 2012 R2
Version: 12.14.8.0 **(Optional)**
Filename: cp028838.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.0.0.25 or later, for use with this driver.

Fixes

This driver addresses an issue that results in the failure of a Powershell command that contains an adapter name.

Enhancements

This product now supports the HPE Ethernet 1Gb 4-port 366i Communication Board.

Supported Devices and Features

This driver supports the following HPE Intel E1R network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361FLB Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366i Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter

- HP Ethernet 1Gb 2-port 367i Adapter

HPE Intel E1R Driver for Windows Server 2016
Version: 12.15.184.0 (B) **(Optional)**
Filename: cp031179.compsig; cp031179.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.0.4 or later, for use with this driver.

Enhancements

Some of the devices supported by this product have been rebranded.

Supported Devices and Features

This driver supports the following HPE Intel E1R network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HPE Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366i Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- HPE Ethernet 1Gb 4-port 366FLR Adapter
- HPE Ethernet 1Gb 4-port 366M Adapter
- HPE Ethernet 1Gb 4-port 366T Adapter

HPE Intel i40e Drivers for Red Hat Enterprise Linux 6 x86_64
Version: 2.4.6.1-4 **(Optional)**
Filename: kmod-hp-i40e-2.4.6.1-4.rhel6u8.x86_64.compsig; kmod-hp-i40e-2.4.6.1-4.rhel6u8.x86_64.rpm; kmod-hp-i40e-2.4.6.1-4.rhel6u9.x86_64.compsig; kmod-hp-i40e-2.4.6.1-4.rhel6u9.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an error seen when a submodule is being updated.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 563i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter

HPE Intel i40e Drivers for Red Hat Enterprise Linux 7 x86_64
Version: 2.4.6.1-4 **(Optional)**
Filename: kmod-hp-i40e-2.4.6.1-4.rhel7u4.x86_64.compsig; kmod-hp-i40e-2.4.6.1-4.rhel7u4.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an error seen when a submodule is being updated.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 563i Adapter
- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter

HPE Intel i40e Drivers for SUSE Linux Enterprise Server 11 x86_64
Version: 2.4.6.1-4 **(Optional)**
Filename: hp-i40e-kmp-default-2.4.6.1_3.0.101_63-4.sles11sp4.x86_64.compsig; hp-i40e-kmp-default-2.4.6.1_3.0.101_63-4.sles11sp4.x86_64.rpm; hp-i40e-kmp-default-2.4.6.1_3.0.76_0.11-4.sles11sp3.x86_64.compsig; hp-i40e-kmp-default-2.4.6.1_3.0.76_0.11-4.sles11sp3.x86_64.rpm; hp-i40e-kmp-xen-2.4.6.1_3.0.101_63-4.sles11sp4.x86_64.compsig; hp-i40e-kmp-xen-2.4.6.1_3.0.101_63-4.sles11sp4.x86_64.rpm; hp-i40e-kmp-xen-2.4.6.1_3.0.76_0.11-4.sles11sp3.x86_64.compsig; hp-i40e-kmp-xen-2.4.6.1_3.0.76_0.11-4.sles11sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an error seen when a submodule is being updated.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 563i Adapter
- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter

HPE Intel i40e Drivers for SUSE Linux Enterprise Server 12 x86_64
Version: 2.4.6.1-4 **(Optional)**
Filename: hp-i40e-kmp-default-2.4.6.1_k4.4.21_69-4.sles12sp2.x86_64.compsig; hp-i40e-kmp-default-2.4.6.1_k4.4.21_69-4.sles12sp2.x86_64.rpm; hp-i40e-kmp-default-2.4.6.1_k4.4.73_5-4.sles12sp3.x86_64.compsig; hp-i40e-kmp-default-2.4.6.1_k4.4.73_5-4.sles12sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an error seen when a submodule is being updated.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 563i Adapter
- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter

HPE Intel i40ea Driver for Windows Server 2012
Version: 1.8.94.0 **(Optional)**

Filename: cp034516.compsig; cp034516.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a Windows Stop Error (BSOD) when the system is operating in a heavily stressed iSCSI environment.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter

HPE Intel i40ea Driver for Windows Server 2012 R2
Version: 1.8.94.0 **(Optional)**
Filename: cp034517.compsig; cp034517.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a Windows Stop Error (BSOD) when the system is operating in a heavily stressed iSCSI environment.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter

HPE Intel i40ea Driver for Windows Server 2016
Version: 1.8.94.0 **(Optional)**
Filename: cp034518.compsig; cp034518.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a Windows Stop Error (BSOD) when the system is operating in a heavily stressed iSCSI environment.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter

HPE Intel i40eb Driver for Windows Server 2012 R2
Version: 1.8.94.0 **(Optional)**
Filename: cp034519.compsig; cp034519.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a Stop Error (0x133) when the system is operating in a heavily stressed environment.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter

HPE Intel i40eb Driver for Windows Server 2016
Version: 1.8.94.0 **(Optional)**
Filename: cp034520.compsig; cp034520.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a Stop Error (0x133) when the system is operating in a heavily stressed environment.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter

HPE Intel i40en Driver for VMware vSphere 6.0
Version: 2018.06.04 **(Optional)**
Filename: cp034656.compsig; cp034656.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for VMware*, version 3.7.8 or later, for use with this driver.

Fixes

This product addresses an issue where system management IP is lost after a firmware update on an HPE Ethernet 10Gb 2-port 562SFP+ Adapter or an HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter

HPE Intel i40en Driver for VMware vSphere 6.5
Version: 2018.06.04 **(Optional)**
Filename: cp034524.compsig; cp034524.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for VMware*, version 3.7.8 or later, for use with this driver.

Fixes

This product addresses an issue where system management IP is lost after a firmware update on an HPE Ethernet 10Gb 2-port 562SFP+ Adapter or an HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter

HPE Intel i40evf Drivers for Red Hat Enterprise Linux 6 x86_64
Version: 3.5.6.1-5 **(Optional)**
Filename: kmod-hp-i40evf-3.5.6.1-5.rhel6u8.x86_64.compsig; kmod-hp-i40evf-3.5.6.1-5.rhel6u8.x86_64.rpm; kmod-hp-i40evf-3.5.6.1-5.rhel6u9.x86_64.compsig; kmod-hp-i40evf-3.5.6.1-5.rhel6u9.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an error seen when a submodule is being updated.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 563i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter

HPE Intel i40evf Drivers for Red Hat Enterprise Linux 7 x86_64
Version: 3.5.6.1-5 **(Optional)**
Filename: kmod-hp-i40evf-3.5.6.1-5.rhel7u4.x86_64.compsig; kmod-hp-i40evf-3.5.6.1-5.rhel7u4.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an error seen when a submodule is being updated.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter

- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 563i Adapter
- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter

HPE Intel i40evf Drivers for SUSE Linux Enterprise Server 11 x86_64
Version: 3.5.6.1-5 **(Optional)**
Filename: hp-i40evf-kmp-default-3.5.6.1_3.0.101_63-5.sles11sp4.x86_64.compsig; hp-i40evf-kmp-default-3.5.6.1_3.0.101_63-5.sles11sp4.x86_64.rpm; hp-i40evf-kmp-default-3.5.6.1_3.0.76_0.11-5.sles11sp3.x86_64.compsig; hp-i40evf-kmp-default-3.5.6.1_3.0.76_0.11-5.sles11sp3.x86_64.rpm; hp-i40evf-kmp-xen-3.5.6.1_3.0.101_63-5.sles11sp4.x86_64.compsig; hp-i40evf-kmp-xen-3.5.6.1_3.0.101_63-5.sles11sp4.x86_64.rpm; hp-i40evf-kmp-xen-3.5.6.1_3.0.76_0.11-5.sles11sp3.x86_64.compsig; hp-i40evf-kmp-xen-3.5.6.1_3.0.76_0.11-5.sles11sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an error seen when a submodule is being updated.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 563i Adapter
- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter

HPE Intel i40evf Drivers for SUSE Linux Enterprise Server 12 x86_64
Version: 3.5.6.1-5 **(Optional)**
Filename: hp-i40evf-kmp-default-3.5.6.1_k4.4.21_69-5.sles12sp2.x86_64.compsig; hp-i40evf-kmp-default-3.5.6.1_k4.4.21_69-5.sles12sp2.x86_64.rpm; hp-i40evf-kmp-default-3.5.6.1_k4.4.73_5-5.sles12sp3.x86_64.compsig; hp-i40evf-kmp-default-3.5.6.1_k4.4.73_5-5.sles12sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an error seen when a submodule is being updated.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 563i Adapter
- HPE Ethernet 1Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter

HPE Intel igb Drivers for Red Hat Enterprise Linux 6 x86_64
Version: 5.3.5.15-4 **(Optional)**
Filename: kmod-hp-igb-5.3.5.15-4.rhel6u8.x86_64.compsig; kmod-hp-igb-5.3.5.15-4.rhel6u8.x86_64.rpm; kmod-hp-igb-5.3.5.15-4.rhel6u9.x86_64.compsig; kmod-hp-igb-5.3.5.15-4.rhel6u9.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Enhancements

This product is updated to maintain compatibility with firmware version 1.15.x.

Supported Devices and Features

These drivers support the following Intel network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter

HPE Intel igb Drivers for Red Hat Enterprise Linux 7 x86_64
Version: 5.3.5.15-4 **(Optional)**
Filename: kmod-hp-igb-5.3.5.15-4.rhel7u4.x86_64.compsig; kmod-hp-igb-5.3.5.15-4.rhel7u4.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Enhancements

This product is updated to maintain compatibility with firmware version 1.15.x.

Supported Devices and Features

These drivers support the following Intel network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter

HPE Intel igb Drivers for SUSE Linux Enterprise Server 11 x86_64
Version: 5.3.5.15-4 **(Optional)**
Filename: hp-igb-kmp-default-5.3.5.15_3.0.101_63-4.sles11sp4.x86_64.compsig; hp-igb-kmp-default-5.3.5.15_3.0.101_63-4.sles11sp4.x86_64.rpm; hp-igb-kmp-default-5.3.5.15_3.0.76_0.11-4.sles11sp3.x86_64.compsig; hp-igb-kmp-default-5.3.5.15_3.0.76_0.11-4.sles11sp3.x86_64.rpm; hp-igb-kmp-xen-5.3.5.15_3.0.101_63-4.sles11sp4.x86_64.compsig; hp-igb-kmp-xen-5.3.5.15_3.0.101_63-4.sles11sp4.x86_64.rpm; hp-igb-kmp-xen-5.3.5.15_3.0.76_0.11-4.sles11sp3.x86_64.compsig; hp-igb-kmp-xen-5.3.5.15_3.0.76_0.11-4.sles11sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Enhancements

This product is updated to maintain compatibility with firmware version 1.15.x.

Supported Devices and Features

These drivers support the following Intel network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter

- HP Ethernet 1Gb 4-port 366i Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter

HPE Intel igb Drivers for SUSE Linux Enterprise Server 12 x86_64
Version: 5.3.5.15-4 **(Optional)**
Filename: hp-igb-kmp-default-5.3.5.15_k4.4.21_69-4.sles12sp2.x86_64.compsig; hp-igb-kmp-default-5.3.5.15_k4.4.21_69-4.sles12sp2.x86_64.rpm; hp-igb-kmp-default-5.3.5.15_k4.4.73_5-4.sles12sp3.x86_64.compsig; hp-igb-kmp-default-5.3.5.15_k4.4.73_5-4.sles12sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Enhancements

This product is updated to maintain compatibility with firmware version 1.15.x.

This product now supports updated kernel of SLES12 SP2.

Supported Devices and Features

These drivers support the following Intel network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter

HPE Intel igbn Driver for VMware vSphere 6.0
Version: 2018.06.04 **(Optional)**
Filename: cp031603.compsig; cp031603.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for VMware*, version 3.7.8 or later, for use with this driver.

Enhancements

This product now contains the native driver, which replaces the vmklinux driver in earlier versions of this product.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HP Ethernet 1Gb 4-port 366i Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter

HPE Intel igbn Driver for VMware vSphere 6.5
Version: 2018.02.12 **(Optional)**
Filename: cp030155.compsig; cp030155.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for VMware*, version 3.6.13 or later, for use with this driver.

Enhancements

Initial release.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HP Ethernet 1Gb 4-port 366i Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter

HPE Intel ixgbe Drivers for Red Hat Enterprise Linux 6 x86_64
Version: 5.3.5.1-5 **(Optional)**
Filename: kmod-hp-ixgbe-5.3.5.1-5.rhel6u8.x86_64.compsig; kmod-hp-ixgbe-5.3.5.1-5.rhel6u8.x86_64.rpm; kmod-hp-ixgbe-5.3.5.1-5.rhel6u9.x86_64.compsig; kmod-hp-ixgbe-5.3.5.1-5.rhel6u9.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an issue with obtaining a link automatically after swapping SFP+ modules of different speeds.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixgbe Drivers for Red Hat Enterprise Linux 7 x86_64
Version: 5.3.5.1-5 **(Optional)**
Filename: kmod-hp-ixgbe-5.3.5.1-5.rhel7u4.x86_64.compsig; kmod-hp-ixgbe-5.3.5.1-5.rhel7u4.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an issue with obtaining a link automatically after swapping SFP+ modules of different speeds.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter

- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixgbe Drivers for SUSE Linux Enterprise Server 11 x86_64
Version: 5.3.5.1-5 **(Optional)**
Filename: hp-ixgbe-kmp-default-5.3.5.1_3.0.101_63-5.sles11sp4.x86_64.compsig; hp-ixgbe-kmp-default-5.3.5.1_3.0.101_63-5.sles11sp4.x86_64.rpm; hp-ixgbe-kmp-default-5.3.5.1_3.0.76_0.11-5.sles11sp3.x86_64.compsig; hp-ixgbe-kmp-default-5.3.5.1_3.0.76_0.11-5.sles11sp3.x86_64.rpm; hp-ixgbe-kmp-xen-5.3.5.1_3.0.101_63-5.sles11sp4.x86_64.compsig; hp-ixgbe-kmp-xen-5.3.5.1_3.0.101_63-5.sles11sp4.x86_64.rpm; hp-ixgbe-kmp-xen-5.3.5.1_3.0.76_0.11-5.sles11sp3.x86_64.compsig; hp-ixgbe-kmp-xen-5.3.5.1_3.0.76_0.11-5.sles11sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an issue with obtaining a link automatically after swapping SFP+ modules of different speeds.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixgbe Drivers for SUSE Linux Enterprise Server 12 x86_64
Version: 5.3.5.1-5 **(Optional)**
Filename: hp-ixgbe-kmp-default-5.3.5.1_k4.4.21_69-5.sles12sp2.x86_64.compsig; hp-ixgbe-kmp-default-5.3.5.1_k4.4.21_69-5.sles12sp2.x86_64.rpm; hp-ixgbe-kmp-default-5.3.5.1_k4.4.73_5-5.sles12sp3.x86_64.compsig; hp-ixgbe-kmp-default-5.3.5.1_k4.4.73_5-5.sles12sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product corrects an issue with obtaining a link automatically after swapping SFP+ modules of different speeds.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixgben Driver for VMware vSphere 6.0
Version: 2018.06.04 **(Optional)**
Filename: cp032893.compsig; cp032893.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for VMware*, version 3.7.8 or later, for use with this driver.

Enhancements

This product now contains the native driver, which replaces the vmklinux driver in earlier versions of this product.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixgben Driver for VMware vSphere 6.5
Version: 2018.02.12 **(Optional)**
Filename: cp030156.compsig; cp030156.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for VMware*, version 3.6.13 or later, for use with this driver.

Enhancements

Initial release.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixgbevf Drivers for Red Hat Enterprise Linux 6 x86_64
Version: 4.3.3.1-5 **(Optional)**
Filename: kmod-hp-ixgbevf-4.3.3.1-5.rhel6u8.x86_64.compsig; kmod-hp-ixgbevf-4.3.3.1-5.rhel6u8.x86_64.rpm; kmod-hp-ixgbevf-4.3.3.1-5.rhel6u9.x86_64.compsig; kmod-hp-ixgbevf-4.3.3.1-5.rhel6u9.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product addresses an issue where the number of supported virtual functions reported by the sriov_totalvfs parameter is incorrect.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter

- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixgbevf Drivers for Red Hat Enterprise Linux 7 x86_64
Version: 4.3.3.1-5 **(Optional)**
Filename: kmod-hp-ixgbevf-4.3.3.1-5.rhel7u4.x86_64.compsig; kmod-hp-ixgbevf-4.3.3.1-5.rhel7u4.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product addresses an issue where the number of supported virtual functions reported by the sriov_totalvfs parameter is incorrect.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixgbevf Drivers for SUSE Linux Enterprise Server 11 x86_64
Version: 4.3.3.1-5 **(Optional)**
Filename: hp-ixgbevf-kmp-default-4.3.3.1_3.0.101_63-5.sles11sp4.x86_64.compsig; hp-ixgbevf-kmp-default-4.3.3.1_3.0.101_63-5.sles11sp4.x86_64.rpm; hp-ixgbevf-kmp-default-4.3.3.1_3.0.76_0.11-5.sles11sp3.x86_64.compsig; hp-ixgbevf-kmp-default-4.3.3.1_3.0.76_0.11-5.sles11sp3.x86_64.rpm; hp-ixgbevf-kmp-xen-4.3.3.1_3.0.101_63-5.sles11sp4.x86_64.compsig; hp-ixgbevf-kmp-xen-4.3.3.1_3.0.101_63-5.sles11sp4.x86_64.rpm; hp-ixgbevf-kmp-xen-4.3.3.1_3.0.76_0.11-5.sles11sp3.x86_64.compsig; hp-ixgbevf-kmp-xen-4.3.3.1_3.0.76_0.11-5.sles11sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product addresses an issue where the number of supported virtual functions reported by the sriov_totalvfs parameter is incorrect.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixgbevf Drivers for SUSE Linux Enterprise Server 12 x86_64
Version: 4.3.3.1-5 **(Optional)**
Filename: hp-ixgbevf-kmp-default-4.3.3.1_k4.4.21_69-5.sles12sp2.x86_64.compsig; hp-ixgbevf-kmp-default-4.3.3.1_k4.4.21_69-5.sles12sp2.x86_64.rpm; hp-ixgbevf-kmp-default-4.3.3.1_k4.4.73_5-5.sles12sp3.x86_64.compsig; hp-ixgbevf-kmp-default-4.3.3.1_k4.4.73_5-5.sles12sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Linux x86_64*, version 1.15.9 or later, for use with these drivers.

Fixes

This product addresses an issue where the number of supported virtual functions reported by the sriov_totalvfs parameter is incorrect.

This product corrects an installation issue on SLES12 SP2.

This product corrects an issue with setting the Maximum Transmission Unit (MTU) size to a value greater than 1500 in SUSE12 SP3.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixn Driver for Windows Server 2012
Version: 3.14.78.0 **(Optional)**
Filename: cp033707.compsig; cp033707.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.2.2 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a link flap with the 1G passthru module.

Supported Devices and Features

This component supports the following network adapters:

- HPE Ethernet 10Gb 2-port 560FLB Adapter
- HPE Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 560SFP+ Adapter HPE
- Ethernet 10Gb 2-port 560M Adapter

HPE Intel ixn Driver for Windows Server 2012 R2
Version: 3.14.78.0 **(Optional)**
Filename: cp033708.compsig; cp033708.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.2.2 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a link flap with the 1G passthru module.

Supported Devices and Features

This component supports the following network adapters:

- HPE Ethernet 10Gb 2-port 560FLB Adapter
- HPE Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 560SFP+ Adapter HPE
- Ethernet 10Gb 2-port 560M Adapter

HPE Intel ixn Driver for Windows Server 2016
Version: 4.1.77.0 **(Optional)**
Filename: cp033706.compsig; cp033706.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.2.2 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a link flap with the 1G passthru module.

Enhancements

This driver is updated to maintain compatibility with latest NDIS drivers.

Supported Devices and Features

This component supports the following network adapters:

- HPE Ethernet 10Gb 2-port 560FLB Adapter
- HPE Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 560SFP+ Adapter HPE
- Ethernet 10Gb 2-port 560M Adapter

HPE Intel ixs Driver for Windows Server 2012 R2
Version: 3.14.75.0 **(Optional)**
Filename: cp033709.compsig; cp033709.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.2.2 or later, for use with this driver.

Enhancements

This driver is updated to maintain compatibility with latest NDIS drivers.

Supported Devices and Features

This driver supports the following network adapters:

- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixs Driver for Windows Server 2016
Version: 4.1.74.0 **(Optional)**
Filename: cp033710.compsig; cp033710.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.2.2 or later, for use with this driver.

Enhancements

This driver is updated to maintain compatibility with latest NDIS drivers.

Supported Devices and Features

This driver supports the following network adapters:

- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter

HPE Intel ixt Driver for Windows Server 2012
Version: 3.14.78.0 **(Optional)**
Filename: cp033711.compsig; cp033711.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.2.2 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a link flap with the 1G passthru module.

Supported Devices and Features

This component supports the following network adapters:

- HPE Ethernet 10Gb 2-port 561FLR-T Adapter
- HPE Ethernet 10Gb 2-port 561T Adapter

HPE Intel ixt Driver for Windows Server 2012 R2
Version: 3.14.78.0 **(Optional)**
Filename: cp033712.compsig; cp033712.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.2.2 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a link flap with the 1G passthru module.

Supported Devices and Features

This component supports the following network adapters:

- HPE Ethernet 10Gb 2-port 561FLR-T Adapter
- HPE Ethernet 10Gb 2-port 561T Adapter

HPE Intel ixt Driver for Windows Server 2016
Version: 4.1.76.0 **(Optional)**
Filename: cp033713.compsig; cp033713.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.2.2 or later, for use with this driver.

Fixes

This driver corrects an issue which results in a link flap with the 1G passthru module.

Supported Devices and Features

This component supports the following network adapters:

- HPE Ethernet 10Gb 2-port 561FLR-T Adapter
- HPE Ethernet 10Gb 2-port 561T Adapter

HPE Intel v40e Driver for Windows Server 2012
Version: 1.5.65.0 (B) **(Optional)**
Filename: cp034521.compsig; cp034521.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Prerequisites

This driver requires host driver version 1.8.90.0 or later.

Fixes

This driver now requires host driver version 1.8.90.0 or later.

Supported Devices and Features

This product supports the following HPE Intel i40ea network adapters:

- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter

HPE Intel v40e Driver for Windows Server 2012 R2
Version: 1.5.76.0 **(Optional)**
Filename: cp034522.compsig; cp034522.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Prerequisites

This driver requires host driver version 1.8.90.0 or later.

Fixes

This driver now requires host driver version 1.8.90.0 or later.

Supported Devices and Features

This product supports the following HPE Intel i40ea network adapters:

- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter

HPE Intel v40e Driver for Windows Server 2016
Version: 1.5.76.0 **(Optional)**
Filename: cp034523.compsig; cp034523.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Prerequisites

This driver requires host driver version 1.8.90.0 or later.

Fixes

This driver now requires host driver version 1.8.90.0 or later.

Supported Devices and Features

This product supports the following HPE Intel i40ea network adapters:

- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter

HPE Intel vxn Driver for Windows Server 2012
Version: 1.0.15.4 **(Optional)**
Filename: cp032567.compsig; cp032567.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.1.0 or later, for use with this driver.

Enhancements

Initial release.

Supported Devices and Features

This component supports the following HPE Intel ixn network adapters:

- HPE Ethernet 10Gb 2-port 560FLB Adapter
- HPE Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 560SFP+ Adapter HPE
- Ethernet 10Gb 2-port 560M Adapter

This component supports the following HPE Intel ixt network adapters:

- HPE Ethernet 10Gb 2-port 561FLR-T Adapter
- HPE Ethernet 10Gb 2-port 561T Adapter

HPE Intel vxn Driver for Windows Server 2012 R2
Version: 1.0.16.1 **(Optional)**
Filename: cp032568.compsig; cp032568.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.1.0 or later, for use with this driver.

Enhancements

Initial release.

Supported Devices and Features

This component supports the following HPE Intel ixn network adapters:

- HPE Ethernet 10Gb 2-port 560FLB Adapter
- HPE Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 560SFP+ Adapter HPE
- Ethernet 10Gb 2-port 560M Adapter

This component supports the following HPE Intel ixt network adapters:

- HPE Ethernet 10Gb 2-port 561FLR-T Adapter
- HPE Ethernet 10Gb 2-port 561T Adapter

HPE Intel vxn Driver for Windows Server 2016
Version: 2.0.210.0 (B) **(Optional)**
Filename: cp034732.compsig; cp034732.exe

Important Note!

HPE recommends the firmware provided in *HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with this driver.

Enhancements

The component installer for this package is now digitally signed.

Supported Devices and Features

This component supports the following HPE Intel ixn network adapters:

- HPE Ethernet 10Gb 2-port 560FLB Adapter
- HPE Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 560SFP+ Adapter HPE
- Ethernet 10Gb 2-port 560M Adapter

This component supports the following HPE Intel ixt network adapters:

- HPE Ethernet 10Gb 2-port 561FLR-T Adapter
- HPE Ethernet 10Gb 2-port 561T Adapter

HPE Mellanox CX3 Driver for Windows Server 2012
Version: 5.35.12978.0 **(Optional)**
Filename: cp031560.compsig; cp031560.exe

Fixes

Fixed an issue where the link speed of an IPoIB adapter was the actual speed and not the official speed (i.e. 54.3GB/s instead of 56 GB/s).
Fixed an issue where firmware burning failed on servers with Connectx-3 and Connectx-4 devices.
Fixed an issue were Mellanox counters in Perfmon did not work over HPE devices.
Fixed an issue that caused the installation process to hang while checking if the RDSH service is installed.
Fixed an issue where a SR-IOV team failure was caused by an unsuccessful adapter parameters update.
Fixed a crash in the driver properties dialog in the case where more than 8 teaming ports were defined.
Fixed an issue which reported a false error for successful netsh tcp settings via performance tuning.
Fixed a crash which could occur during virtual function initialization.
Deactivated the RDMA statistics counters query for vPorts for which RDMA is not enabled.

Fixed the issue which caused the failure of the powershell command Get_MLNXNetAdapterSettings and the command Get_MLNXNetAdapterFlowControlSettings on servers with Connectx3/Pro and ConnectX4/LX devices.
Fixed a crash which could occur during driver initializtion.
Fixed an issue that generated and sent an erroneous message to the Windows event log when using firmware 2.36.5000 whenever "Mellanox WinOF Bus Counters" was selected in Perfmon.
Fixed an issue that occasionally caused system-hang when TCP offload parameters were updated dynamically while SR-IOV was enabled.
Fixed an issue that occasionally caused system-hang upon bus driver disabling, when the encapsulation parameters were updated dynamically while SR-IOV was enabled.
Fixed an issue where the virtual function RDMA was not functional when vSwitch was attached to port 2. Now RDMA over VF is supported only when the vSwitch is attached to port 1.
Fixed an issue which caused the driver to hang during installation process.

Supported Devices and Features

This driver supports the following HPE Mellanox CX3 network adapters:

- HP Ethernet 10G 2-port 546FLR-SFP+ Adapter
- HP Ethernet 10G 2-port 546SFP+ Adapter
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP Adapter
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M Adapter
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP Adapter
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+M Adapter
- HP InfiniBand QDR/EN 10Gb Dual Port 544FLR-QSFP Adapter
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544QSFP Adapter
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544FLR-QSFP Adapter
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544M Adapter
- HP InfiniBand QDR/EN 10Gb Dual Port 544M Adapter
- HP Infiniband QDR/Ethernet 10Gb 2P 544i Adapter

HPE Mellanox CX3 Driver for Windows Server 2012 R2
Version: 5.35.12978.0 **(Optional)**
Filename: cp031561.compsig; cp031561.exe

Fixes

Fixed an issue where the link speed of an IPoIB adapter was the actual speed and not the official speed (i.e. 54.3GB/s instead of 56 GB/s).
Fixed an issue where firmware burning failed on servers with Connectx-3 and Connectx-4 devices.
Fixed an issue were Mellanox counters in Perfmon did not work over HPE devices.
Fixed an issue that caused the installation process to hang while checking if the RDSH service is installed.
Fixed an issue where a SR-IOV team failure was caused by an unsuccessful adapter parameters update.
Fixed a crash in the driver properties dialog in the case where more than 8 teaming ports were defined.
Fixed an issue which reported a false error for successful netsh tcp settings via performance tuning.
Fixed a crash which could occur during virtual function initialization.
Deactivated the RDMA statistics counters query for vPorts for which RDMA is not enabled.
Fixed the issue which caused the failure of the powershell command Get_MLNXNetAdapterSettings and the command Get_MLNXNetAdapterFlowControlSettings on servers with Connectx3/Pro and ConnectX4/LX devices.
Fixed a crash which could occur during driver initialization.
Fixed an issue that generated and sent an erroneous message to the Windows event log when using firmware 2.36.5000 whenever "Mellanox WinOF Bus Counters" was selected in Perfmon.
Fixed an issue that occasionally caused system-hang when TCP offload parameters were updated dynamically while SR-IOV was enabled.
Fixed an issue that occasionally caused system-hang upon bus driver disabling, when the encapsulation parameters were updated dynamically while SR-IOV was enabled.
Fixed an issue where the virtual function RDMA was not functional when vSwitch was attached to port 2. Now RDMA over VF is supported only when the vSwitch is attached to port 1.
Fixed an issue which caused the driver to hang during installation process.

Supported Devices and Features

This driver supports the following HPE Mellanox CX3 network adapters:

- HP Ethernet 10G 2-port 546FLR-SFP+ Adapter
- HP Ethernet 10G 2-port 546SFP+ Adapter
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP Adapter
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M Adapter
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP Adapter
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+M Adapter
- HP InfiniBand QDR/EN 10Gb Dual Port 544FLR-QSFP Adapter
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544QSFP Adapter
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544FLR-QSFP Adapter
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544M Adapter
- HP InfiniBand QDR/EN 10Gb Dual Port 544M Adapter
- HP Infiniband QDR/Ethernet 10Gb 2P 544i Adapter

HPE Mellanox CX3 Driver for Windows Server 2016
Version: 5.35.12978.0 **(Optional)**
Filename: cp031850.compsig; cp031850.exe

Fixes

Fixed an issue where the link speed of an IPoIB adapter was the actual speed and not the official speed (i.e. 54.3GB/s instead of 56 GB/s).
Fixed an issue where firmware burning failed on servers with Connectx-3 and Connectx-4 devices.
Fixed an issue were Mellanox counters in Perfmon did not work over HPE devices.
Fixed an issue that caused the installation process to hang while checking if the RDSH service is installed.
Fixed an issue where a SR-IOV team failure was caused by an unsuccessful adapter parameters update.
Fixed a crash in the driver properties dialog in the case where more than 8 teaming ports were defined.
Fixed an issue which reported a false error for successful netsh tcp settings via performance tuning.
Fixed a crash which could occur during virtual function initialization.
Deactivated the RDMA statistics counters query for vPorts for which RDMA is not enabled.
Fixed an issue that caused occasional failures of the execution of OID_QOS_OFFLOAD_CURRENT_CAPABILITIES on Windows 2016.
Fixed an issue that caused traffic loss following an upgrade of Windows 2016 virtual machine.
Fixed the issue which caused the failure of the powershell command Get_MLNXNetAdapterSettings and the command Get_MLNXNetAdapterFlowControlSettings on servers with Connectx3/Pro and ConnectX4/LX devices.
Fixed a crash which could occur during driver initialization.
Fixed an issue that generated and sent an erroneous message to the Windows event log when using firmware 2.36.5000 whenever "Mellanox WinOF Bus Counters" was selected in Perfmon.
Fixed an issue that occasionally caused system-hang when TCP offload parameters were updated dynamically while SR-IOV was enabled.
Fixed an issue that occasionally caused system-hang upon bus driver disabling, when the encapsulation parameters were updated dynamically while SR-IOV was enabled.
Fixed an issue where the virtual function RDMA was not functional when vSwitch was attached to port 2. Now RDMA over VF is supported only when the vSwitch is attached to port 1.
Fixed an issue which caused the driver to hang during installation process.

Supported Devices and Features

This driver supports the following HP Mellanox CX3 network adapters:

- HP Ethernet 10G 2-port 546FLR-SFP+ Adapter
- HP Ethernet 10G 2-port 546SFP+ Adapter
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP Adapter
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M Adapter
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP Adapter
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+M Adapter
- HP InfiniBand QDR/EN 10Gb Dual Port 544FLR-QSFP Adapter
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544QSFP Adapter
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544FLR-QSFP Adapter
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544M Adapter
- HP InfiniBand QDR/EN 10Gb Dual Port 544M Adapter
- HP Infiniband QDR/Ethernet 10Gb 2P 544i Adapter

HPE Mellanox CX4LX and CX5 Driver for Windows Server 2012
Version: 1.90.19216.0 **(Optional)**
Filename: cp034467.compsig; cp034467.exe

Fixes

This driver corrects an issue that results in a firmware hang during virtual machine migration in SR-IOV mode or upon host driver restart.
This driver addresses certification issues that occurr when running ConnectX-4 Lx at 25Gb/s link speed.
This driver corrects an issue which results in a system crash (BSOD) when network traffic is switched from a single receive queue (RQ) to RSS.
This driver corrects an issue which results in system crash (BSOD) when using iSCSI boot with IPoIB under Windows Server 2016.
This driver corrects an issue which results in system crash (BSOD) when sending packets with the *TransmitBuffers" parameter set to a value that is not a power of 2.
This driver corrects an issue which results in IP configuration being reset after uninstalling the driver.
This driver corrects an issue which results in the device reporting more than the supported number of schedule queues. This driver addresses an issue which results in loss of a connectivity when the firmware is upgraded to a version newer than 12/14/16.21.2010 without the driver being upgraded first.

Enhancements

This driver now supports the following network adapters:

- HPE Synergy 6410C 25/50Gb Ethernet Adapter
- HPE Ethernet 100Gb 1-port 842QSFP28 Adapter
- HPE Infiniband FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter
- HPE Infiniband EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter

Supported Devices and Features

This driver supports the following network adapters:

- HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter
- HPE Ethernet 25Gb 2-port 640SFP28 Adapter HPE
- Synergy 6410C 25/50Gb Ethernet Adapter
- HPE Infiniband FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter
- HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter
- HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter
- HPE Infiniband EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter
- HPE Ethernet 100Gb 1-port 842QSFP28 Adapter

HPE Mellanox CX4LX and CX5 Driver for Windows Server 2012 R2
Version: 1.90.19216.0 **(Optional)**
Filename: cp034468.compsig; cp034468.exe

Fixes

This driver corrects an issue that results in a firmware hang during virtual machine migration in SR-IOV mode or upon host driver restart.
This driver addresses certification issues that occurr when running ConnectX-4 Lx at 25Gb/s link speed.
This driver corrects an issue which results in a system crash (BSOD) when network traffic is switched from a single receive queue (RQ) to RSS.
This driver corrects an issue which results in system crash (BSOD) when using iSCSI boot with IPoIB under Windows Server 2016.
This driver corrects an issue which results in system crash (BSOD) when sending packets with the *TransmitBuffers" parameter set to a value that is not a power of 2.
This driver corrects an issue which results in IP configuration being reset after uninstalling the driver.
This driver corrects an issue which results in the device reporting more than the supported number of schedule queues. This driver addresses an issue which results in loss of a connectivity when the firmware is upgraded to a version newer than 12/14/16.21.2010 without the driver being upgraded first.

Enhancements

This driver now supports the following network adapters:

- HPE Synergy 6410C 25/50Gb Ethernet Adapter
- HPE Ethernet 100Gb 1-port 842QSFP28 Adapter
- HPE Infiniband FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter
- HPE Infiniband EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter

Supported Devices and Features

This driver supports the following network adapters:

- HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter
- HPE Ethernet 25Gb 2-port 640SFP28 Adapter HPE
- Synergy 6410C 25/50Gb Ethernet Adapter
- HPE Infiniband FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter
- HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter
- HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter
- HPE Infiniband EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter
- HPE Ethernet 100Gb 1-port 842QSFP28 Adapter

HPE Mellanox CX4LX and CX5 Driver for Windows Server 2016
Version: 1.90.19216.0 **(Optional)**
Filename: cp034469.compsig; cp034469.exe

Fixes

This driver corrects an issue that results in a firmware hang during virtual machine migration in SR-IOV mode or upon host driver restart.
This driver addresses certification issues that occurr when running ConnectX-4 Lx at 25Gb/s link speed.
This driver corrects an issue which results in a system crash (BSOD) when network traffic is switched from a single receive queue (RQ) to RSS.
This driver corrects an issue which results in system crash (BSOD) when using iSCSI boot with IPoIB under Windows Server 2016.
This driver corrects an issue which results in system crash (BSOD) when sending packets with the *TransmitBuffers" parameter set to a value that is not a power of 2.
This driver corrects an issue which results in IP configuration being reset after uninstalling the driver.
This driver corrects an issue which results in the device reporting more than the supported number of schedule queues. This driver addresses an issue which results in loss of a connectivity when the firmware is upgraded to a version newer than 12/14/16.21.2010 without the driver being upgraded first.

Enhancements

This driver now supports the following network adapters:

- HPE Synergy 6410C 25/50Gb Ethernet Adapter
- HPE Ethernet 100Gb 1-port 842QSFP28 Adapter

- HPE Infiniband FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter
- HPE Infiniband EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter

Supported Devices and Features

This driver supports the following network adapters:

- HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter
- HPE Ethernet 25Gb 2-port 640SFP28 Adapter HPE
- Synergy 6410C 25/50Gb Ethernet Adapter
- HPE Infiniband FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter
- HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter
- HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter
- HPE Infiniband EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter
- HPE Ethernet 100Gb 1-port 842QSFP28 Adapter

HPE Mellanox RoCE (RDMA over Converged Ethernet) Driver for Red Hat Enterprise Linux 6 Update 8 (x86_64)
Version: 4.3 **(Recommended)**
Filename: kmod-mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.rhel6u8.x86_64.compsig; kmod-mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.rhel6u8.x86_64.rpm; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.rhel6u8.x86_64.compsig; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.rhel6u8.x86_64.rpm

Important Note!

Mellanox Ethernet + RoCE Linux driver (mlnx-ofa_kernel RPMs) supports only Ethernet mode of operation for HPE Mellanox adapters. For customers requiring complete InfiniBand functionality or "InfiniBand + Ethernet" modes of operation on the same node, install MLNX-OFED drivers from "Mellanox OFED VPI Drivers and Utilities" Linux Software Delivery Repository (https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/).

Fixes

The following issues have been fixed in version 4.3:

- Sending Work Requests (WRs) with multiple entries where the first entry was less than 18 bytes used to fail.
- When the interface was down, ethtool counters ceased to increase. As a result, RoCE traffic counters were not always incremented.
- Compilation errors of MLNX_OFED over kernel when CONFIG_PTP_1588_CLOCK parameter was not set.
- System used to hang when trying to allocate multiple device memory buffers from different processes simultaneously.

Enhancements

Changes and new features in HPE Mellanox RoCE driver version 4.3:

- For ConnectX-5 adapters, added support for the following multi-packet Work Requests related verbs for control path:
  - ibv_exp_query_device
  - ibv_exp_create_srq
- Added support for the following new features:
  - RDMA atomic commands offload so that when an RDMA write operation is issued, the payload indicates which atomic operation to perform, instead of being written to the Memory Region (MR).
  - Out of box RoCE LAG support for Red Hat Enterprise Linux 7 Update 2 and Red Hat Enterprise Linux 6 Update 9.
  - A new counter rx_steer_missed_packets which provides the number of packets that were received by the NIC, yet were discarded/dropped since they did not match any flow in the NIC steering flow table.
  - Ability for SR-IOV counter rx_dropped to count the number of packets that were dropped while vport was down.
  - RSYNC feature to ensure correct ordering of memory operations between the GPU and HCA.
  - Triggering software reset for firmware/driver recovery. When fatal errors occur, firmware can be reset and driver reloaded.
  - Option to retrieve the Hardware timestamp when polling for completions from a completion queue that is attached to a multi-packet RQ (Striding RQ).
  - The following advanced burst control parameters:
    - max_burst_sz - for indicating the maximal burst size of packets
    - typical_pkt_sz - for improving the accuracy of the rate limiter
- Removed support for Virtual MAC feature.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 6U8 (x86_64) supported by this binary rpm are:
2.6.32-642.el6 - (x86_64) and future update kernels.

HPE Mellanox RoCE (RDMA over Converged Ethernet) Driver for Red Hat Enterprise Linux 6 Update 9 (x86_64)
Version: 4.3 **(Recommended)**
Filename: kmod-mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.rhel6u9.x86_64.compsig; kmod-mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.rhel6u9.x86_64.rpm; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.rhel6u9.x86_64.compsig; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.rhel6u9.x86_64.rpm

Important Note!

Mellanox Ethernet + RoCE Linux driver (mlnx-ofa_kernel RPMs) supports only Ethernet mode of operation for HPE Mellanox adapters. For customers requiring complete InfiniBand functionality or "InfiniBand + Ethernet" modes of operation on the same node, install MLNX-OFED drivers from "Mellanox OFED VPI Drivers and Utilities" Linux Software Delivery Repository (https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/).

Fixes

The following issues have been fixed in version 4.3:

- Sending Work Requests (WRs) with multiple entries where the first entry was less than 18 bytes used to fail.
- When the interface was down, ethtool counters ceased to increase. As a result, RoCE traffic counters were not always incremented.
- Compilation errors of MLNX_OFED over kernel when CONFIG_PTP_1588_CLOCK parameter was not set.
- System used to hang when trying to allocate multiple device memory buffers from different processes simultaneously.

Enhancements

Changes and new features in HPE Mellanox RoCE driver version 4.3:

- For ConnectX-5 adapters, added support for the following multi-packet Work Requests related verbs for control path:
  - ibv_exp_query_device
  - ibv_exp_create_srq
- Added support for the following new features:
  - RDMA atomic commands offload so that when an RDMA write operation is issued, the payload indicates which atomic operation to perform, instead of being written to the Memory Region (MR).
  - Out of box RoCE LAG support for Red Hat Enterprise Linux 7 Update 2 and Red Hat Enterprise Linux 6 Update 9.
  - A new counter rx_steer_missed_packets which provides the number of packets that were received by the NIC, yet were discarded/dropped since they did not match any flow in the NIC steering flow table.
  - Ability for SR-IOV counter rx_dropped to count the number of packets that were dropped while vport was down.
  - RSYNC feature to ensure correct ordering of memory operations between the GPU and HCA.
  - Triggering software reset for firmware/driver recovery. When fatal errors occur, firmware can be reset and driver reloaded.
  - Option to retrieve the Hardware timestamp when polling for completions from a completion queue that is attached to a multi-packet RQ (Striding RQ).
  - The following advanced burst control parameters:
    - max_burst_sz - for indicating the maximal burst size of packets
    - typical_pkt_sz - for improving the accuracy of the rate limiter
- Removed support for Virtual MAC feature.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 6 Update 9 (x86_64) supported by this binary rpm are:
2.6.32-696.el6 - (x86_64) and future update kernels.

HPE Mellanox RoCE (RDMA over Converged Ethernet) Driver for Red Hat Enterprise Linux 7 Update 3 (x86_64)
Version: 4.3 **(Recommended)**
Filename: kmod-mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.rhel7u3.x86_64.compsig; kmod-mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.rhel7u3.x86_64.rpm; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.rhel7u3.x86_64.compsig; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.rhel7u3.x86_64.rpm

Important Note!

Mellanox Ethernet + RoCE Linux driver (mlnx-ofa_kernel RPMs) supports only Ethernet mode of operation for HPE Mellanox adapters. For customers requiring complete InfiniBand functionality or "InfiniBand + Ethernet" modes of operation on the same node, install MLNX-OFED drivers from "Mellanox OFED VPI Drivers and Utilities" Linux Software Delivery Repository (https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/).

Fixes

The following issues have been fixed in version 4.3:

- Sending Work Requests (WRs) with multiple entries where the first entry was less than 18 bytes used to fail.
- When the interface was down, ethtool counters ceased to increase. As a result, RoCE traffic counters were not always incremented.
- Compilation errors of MLNX_OFED over kernel when CONFIG_PTP_1588_CLOCK parameter was not set.
- System used to hang when trying to allocate multiple device memory buffers from different processes simultaneously.

Enhancements

Changes and new features in HPE Mellanox RoCE driver version 4.3:

- For ConnectX-5 adapters, added support for the following multi-packet Work Requests related verbs for control path:
  - ibv_exp_query_device
  - ibv_exp_create_srq
- Added support for the following new features:
  - RDMA atomic commands offload so that when an RDMA write operation is issued, the payload indicates which atomic operation to perform, instead of being written to the Memory Region (MR).
  - Out of box RoCE LAG support for Red Hat Enterprise Linux 7 Update 2 and Red Hat Enterprise Linux 6 Update 9.

        - A new counter rx_steer_missed_packets which provides the number of packets that were received by the NIC, yet were discarded/dropped since they did not match any flow in the NIC steering flow table.
        - Ability for SR-IOV counter rx_dropped to count the number of packets that were dropped while vport was down.
        - RSYNC feature to ensure correct ordering of memory operations between the GPU and HCA.
        - Triggering software reset for firmware/driver recovery. When fatal errors occur, firmware can be reset and driver reloaded.
        - Option to retrieve the Hardware timestamp when polling for completions from a completion queue that is attached to a multi-packet RQ (Striding RQ).
        - The following advanced burst control parameters:
            - max_burst_sz - for indicating the maximal burst size of packets
            - typical_pkt_sz - for improving the accuracy of the rate limiter
    - Removed support for Virtual MAC feature.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 7 Update 3 (x86_64) supported by this binary rpm are:
3.10.0-514.el7 - (x86_64) and future update kernels.

HPE Mellanox RoCE (RDMA over Converged Ethernet) Driver for Red Hat Enterprise Linux 7 Update 4 (x86_64)
Version: 4.3 **(Recommended)**
Filename: kmod-mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.rhel7u4.x86_64.compsig; kmod-mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.rhel7u4.x86_64.rpm; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.rhel7u4.x86_64.compsig; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.rhel7u4.x86_64.rpm

Important Note!

Mellanox Ethernet + RoCE Linux driver (mlnx-ofa_kernel RPMs) supports only Ethernet mode of operation for HPE Mellanox adapters. For customers requiring complete InfiniBand functionality or "InfiniBand + Ethernet" modes of operation on the same node, install MLNX-OFED drivers from "Mellanox OFED VPI Drivers and Utilities" Linux Software Delivery Repository (https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/).

Fixes

The following issues have been fixed in version 4.3:

- Sending Work Requests (WRs) with multiple entries where the first entry was less than 18 bytes used to fail.
- When the interface was down, ethtool counters ceased to increase. As a result, RoCE traffic counters were not always incremented.
- Compilation errors of MLNX_OFED over kernel when CONFIG_PTP_1588_CLOCK parameter was not set.
- System used to hang when trying to allocate multiple device memory buffers from different processes simultaneously.

Enhancements

Changes and new features in HPE Mellanox RoCE driver version 4.3:

- For ConnectX-5 adapters, added support for the following multi-packet Work Requests related verbs for control path:
    - ibv_exp_query_device
    - ibv_exp_create_srq
- Added support for the following new features:
    - RDMA atomic commands offload so that when an RDMA write operation is issued, the payload indicates which atomic operation to perform, instead of being written to the Memory Region (MR).
    - Out of box RoCE LAG support for Red Hat Enterprise Linux 7 Update 2 and Red Hat Enterprise Linux 6 Update 9.
    - A new counter rx_steer_missed_packets which provides the number of packets that were received by the NIC, yet were discarded/dropped since they did not match any flow in the NIC steering flow table.
    - Ability for SR-IOV counter rx_dropped to count the number of packets that were dropped while vport was down.
    - RSYNC feature to ensure correct ordering of memory operations between the GPU and HCA.
    - Triggering software reset for firmware/driver recovery. When fatal errors occur, firmware can be reset and driver reloaded.
    - Option to retrieve the Hardware timestamp when polling for completions from a completion queue that is attached to a multi-packet RQ (Striding RQ).
    - The following advanced burst control parameters:
        - max_burst_sz - for indicating the maximal burst size of packets
        - typical_pkt_sz - for improving the accuracy of the rate limiter
- Removed support for Virtual MAC feature.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 7 Update 4 (x86_64) supported by this binary rpm are:
3.10.0-693.el7 - (x86_64) and future update kernels.

HPE Mellanox RoCE (RDMA over Converged Ethernet) Driver for SUSE LINUX Enterprise Server 11 SP3 AMD64/EM64T)
Version: 4.3 **(Recommended)**
Filename: mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.sles11sp3.x86_64.compsig; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.sles11sp3.x86_64.rpm; mlnx-ofa_kernel-kmp-default-4.3_3.0.76_0.11-OFED.4.3.1.0.1.1.g8509e41.sles11sp3.x86_64.compsig; mlnx-ofa_kernel-kmp-default-4.3_3.0.76_0.11-

OFED.4.3.1.0.1.1.g8509e41.sles11sp3.x86_64.rpm; mlnx-ofa_kernel-kmp-xen-4.3_3.0.76_0.11-OFED.4.3.1.0.1.1.g8509e41.sles11sp3.x86_64.compsig; mlnx-ofa_kernel-kmp-xen-4.3_3.0.76_0.11-OFED.4.3.1.0.1.1.g8509e41.sles11sp3.x86_64.rpm

Important Note!

Mellanox Ethernet + RoCE Linux driver (mlnx-ofa_kernel RPMs) supports only Ethernet mode of operation for HPE Mellanox adapters. For customers requiring complete InfiniBand functionality or "InfiniBand + Ethernet" modes of operation on the same node, install MLNX-OFED drivers from "Mellanox OFED VPI Drivers and Utilities" Linux Software Delivery Repository (https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/).

Fixes

The following issues have been fixed in version 4.3:

- Sending Work Requests (WRs) with multiple entries where the first entry was less than 18 bytes used to fail.
- When the interface was down, ethtool counters ceased to increase. As a result, RoCE traffic counters were not always incremented.
- Compilation errors of MLNX_OFED over kernel when CONFIG_PTP_1588_CLOCK parameter was not set.
- System used to hang when trying to allocate multiple device memory buffers from different processes simultaneously.

Enhancements

Changes and new features in HPE Mellanox RoCE driver version 4.3:

- For ConnectX-5 adapters, added support for the following multi-packet Work Requests related verbs for control path:
  - ibv_exp_query_device
  - ibv_exp_create_srq
- Added support for the following new features:
  - RDMA atomic commands offload so that when an RDMA write operation is issued, the payload indicates which atomic operation to perform, instead of being written to the Memory Region (MR).
  - Out of box RoCE LAG support for Red Hat Enterprise Linux 7 Update 2 and Red Hat Enterprise Linux 6 Update 9.
  - A new counter rx_steer_missed_packets which provides the number of packets that were received by the NIC, yet were discarded/dropped since they did not match any flow in the NIC steering flow table.
  - Ability for SR-IOV counter rx_dropped to count the number of packets that were dropped while vport was down.
  - RSYNC feature to ensure correct ordering of memory operations between the GPU and HCA.
  - Triggering software reset for firmware/driver recovery. When fatal errors occur, firmware can be reset and driver reloaded.
  - Option to retrieve the Hardware timestamp when polling for completions from a completion queue that is attached to a multi-packet RQ (Striding RQ).
  - The following advanced burst control parameters:
    - max_burst_sz - for indicating the maximal burst size of packets
    - typical_pkt_sz - for improving the accuracy of the rate limiter
- Removed support for Virtual MAC feature.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 11 SP3 (AMD64/EM64T) supported by this binary rpm are:
3.0.76-0.11-default - (AMD64/EM64T) and future update kernels.
3.0.76-0.11-xen - (AMD64/EM64T) and future update kernels.

HPE Mellanox RoCE (RDMA over Converged Ethernet) Driver for SUSE LINUX Enterprise Server 11 SP4 AMD64/EM64T)
Version: 4.3 **(Recommended)**
Filename: mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.sles11sp4.x86_64.compsig; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.sles11sp4.x86_64.rpm; mlnx-ofa_kernel-kmp-default-4.3_3.0.101_63-OFED.4.3.1.0.1.1.g8509e41.sles11sp4.x86_64.compsig; mlnx-ofa_kernel-kmp-default-4.3_3.0.101_63-OFED.4.3.1.0.1.1.g8509e41.sles11sp4.x86_64.rpm; mlnx-ofa_kernel-kmp-xen-4.3_3.0.101_63-OFED.4.3.1.0.1.1.g8509e41.sles11sp4.x86_64.compsig; mlnx-ofa_kernel-kmp-xen-4.3_3.0.101_63-OFED.4.3.1.0.1.1.g8509e41.sles11sp4.x86_64.rpm

Important Note!

Mellanox Ethernet + RoCE Linux driver (mlnx-ofa_kernel RPMs) supports only Ethernet mode of operation for HPE Mellanox adapters. For customers requiring complete InfiniBand functionality or "InfiniBand + Ethernet" modes of operation on the same node, install MLNX-OFED drivers from "Mellanox OFED VPI Drivers and Utilities" Linux Software Delivery Repository (https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/).

Fixes

The following issues have been fixed in version 4.3:

- Sending Work Requests (WRs) with multiple entries where the first entry was less than 18 bytes used to fail.
- When the interface was down, ethtool counters ceased to increase. As a result, RoCE traffic counters were not always incremented.
- Compilation errors of MLNX_OFED over kernel when CONFIG_PTP_1588_CLOCK parameter was not set.
- System used to hang when trying to allocate multiple device memory buffers from different processes simultaneously.

Enhancements

Changes and new features in HPE Mellanox RoCE driver version 4.3:

- For ConnectX-5 adapters, added support for the following multi-packet Work Requests related verbs for control path:
  - ibv_exp_query_device
  - ibv_exp_create_srq
- Added support for the following new features:
  - RDMA atomic commands offload so that when an RDMA write operation is issued, the payload indicates which atomic operation to perform, instead of being written to the Memory Region (MR).
  - Out of box RoCE LAG support for Red Hat Enterprise Linux 7 Update 2 and Red Hat Enterprise Linux 6 Update 9.
  - A new counter rx_steer_missed_packets which provides the number of packets that were received by the NIC, yet were discarded/dropped since they did not match any flow in the NIC steering flow table.
  - Ability for SR-IOV counter rx_dropped to count the number of packets that were dropped while vport was down.
  - RSYNC feature to ensure correct ordering of memory operations between the GPU and HCA.
  - Triggering software reset for firmware/driver recovery. When fatal errors occur, firmware can be reset and driver reloaded.
  - Option to retrieve the Hardware timestamp when polling for completions from a completion queue that is attached to a multi-packet RQ (Striding RQ).
  - The following advanced burst control parameters:
    - max_burst_sz - for indicating the maximal burst size of packets
    - typical_pkt_sz - for improving the accuracy of the rate limiter
- Removed support for Virtual MAC feature.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 11 SP4 (AMD64/EM64T) supported by this binary rpm are:
3.0.101-63-default - (AMD64/EM64T) and future update kernels.
3.0.101-63-xen - (AMD64/EM64T) and future update kernels.

HPE Mellanox RoCE (RDMA over Converged Ethernet) Driver for SUSE LINUX Enterprise Server 12 SP2 (AMD64/EM64T)
Version: 4.3 **(Recommended)**
Filename: mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.sles12sp2.x86_64.compsig; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.sles12sp2.x86_64.rpm; mlnx-ofa_kernel-kmp-default-4.3_k4.4.21_69-OFED.4.3.1.0.1.1.g8509e41.sles12sp2.x86_64.compsig; mlnx-ofa_kernel-kmp-default-4.3_k4.4.21_69-OFED.4.3.1.0.1.1.g8509e41.sles12sp2.x86_64.rpm

Important Note!

Mellanox Ethernet + RoCE Linux driver (mlnx-ofa_kernel RPMs) supports only Ethernet mode of operation for HPE Mellanox adapters. For customers requiring complete InfiniBand functionality or "InfiniBand + Ethernet" modes of operation on the same node, install MLNX-OFED drivers from "Mellanox OFED VPI Drivers and Utilities" Linux Software Delivery Repository (https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/).

Fixes

The following issues have been fixed in version 4.3:

- Sending Work Requests (WRs) with multiple entries where the first entry was less than 18 bytes used to fail.
- When the interface was down, ethtool counters ceased to increase. As a result, RoCE traffic counters were not always incremented.
- Compilation errors of MLNX_OFED over kernel when CONFIG_PTP_1588_CLOCK parameter was not set.
- System used to hang when trying to allocate multiple device memory buffers from different processes simultaneously.

Enhancements

Changes and new features in HPE Mellanox RoCE driver version 4.3:

- For ConnectX-5 adapters, added support for the following multi-packet Work Requests related verbs for control path:
  - ibv_exp_query_device
  - ibv_exp_create_srq
- Added support for the following new features:
  - RDMA atomic commands offload so that when an RDMA write operation is issued, the payload indicates which atomic operation to perform, instead of being written to the Memory Region (MR).
  - Out of box RoCE LAG support for Red Hat Enterprise Linux 7 Update 2 and Red Hat Enterprise Linux 6 Update 9.
  - A new counter rx_steer_missed_packets which provides the number of packets that were received by the NIC, yet were discarded/dropped since they did not match any flow in the NIC steering flow table.
  - Ability for SR-IOV counter rx_dropped to count the number of packets that were dropped while vport was down.
  - RSYNC feature to ensure correct ordering of memory operations between the GPU and HCA.
  - Triggering software reset for firmware/driver recovery. When fatal errors occur, firmware can be reset and driver reloaded.
  - Option to retrieve the Hardware timestamp when polling for completions from a completion queue that is attached to a multi-packet RQ (Striding RQ).
    The following advanced burst control parameters:
    max_burst_sz - for indicating the maximal burst size of packets
    typical_pkt_sz - for improving the accuracy of the rate limiter
  Removed support for Virtual MAC feature.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 12 SP2 (AMD64/EM64T) supported by this binary rpm are:
4.4.21-69-default - (AMD64/EM64T) and future update kernels.

HPE Mellanox RoCE (RDMA over Converged Ethernet) Driver for SUSE LINUX Enterprise Server 12 SP3 (AMD64/EM64T)
Version: 4.3 **(Recommended)**
Filename: mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.sles12sp3.x86_64.compsig; mlnx-ofa_kernel-4.3-OFED.4.3.1.0.1.1.g8509e41.3.sles12sp3.x86_64.rpm; mlnx-ofa_kernel-kmp-default-4.3_k4.4.73_5-OFED.4.3.1.0.1.1.g8509e41.sles12sp3.x86_64.compsig; mlnx-ofa_kernel-kmp-default-4.3_k4.4.73_5-OFED.4.3.1.0.1.1.g8509e41.sles12sp3.x86_64.rpm

Important Note!

Mellanox Ethernet + RoCE Linux driver (mlnx-ofa_kernel RPMs) supports only Ethernet mode of operation for HPE Mellanox adapters. For customers requiring complete InfiniBand functionality or "InfiniBand + Ethernet" modes of operation on the same node, install MLNX-OFED drivers from "Mellanox OFED VPI Drivers and Utilities" Linux Software Delivery Repository (https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/).

Fixes

The following issues have been fixed in version 4.3:

- Sending Work Requests (WRs) with multiple entries where the first entry was less than 18 bytes used to fail.
- When the interface was down, ethtool counters ceased to increase. As a result, RoCE traffic counters were not always incremented.
- Compilation errors of MLNX_OFED over kernel when CONFIG_PTP_1588_CLOCK parameter was not set.
- System used to hang when trying to allocate multiple device memory buffers from different processes simultaneously.

Enhancements

Changes and new features in HPE Mellanox RoCE driver version 4.3:

- For ConnectX-5 adapters, added support for the following multi-packet Work Requests related verbs for control path:
  - ibv_exp_query_device
  - ibv_exp_create_srq
- Added support for the following new features:
  - RDMA atomic commands offload so that when an RDMA write operation is issued, the payload indicates which atomic operation to perform, instead of being written to the Memory Region (MR).
  - Out of box RoCE LAG support for Red Hat Enterprise Linux 7 Update 2 and Red Hat Enterprise Linux 6 Update 9.
  - A new counter rx_steer_missed_packets which provides the number of packets that were received by the NIC, yet were discarded/dropped since they did not match any flow in the NIC steering flow table.
  - Ability for SR-IOV counter rx_dropped to count the number of packets that were dropped while vport was down.
  - RSYNC feature to ensure correct ordering of memory operations between the GPU and HCA.
  - Triggering software reset for firmware/driver recovery. When fatal errors occur, firmware can be reset and driver reloaded.
  - Option to retrieve the Hardware timestamp when polling for completions from a completion queue that is attached to a multi-packet RQ (Striding RQ).
  - The following advanced burst control parameters:
    - max_burst_sz - for indicating the maximal burst size of packets
    - typical_pkt_sz - for improving the accuracy of the rate limiter
- Removed support for Virtual MAC feature.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 12 SP3 (AMD64/EM64T) supported by this binary rpm are:
4.4.73-5-default - (AMD64/EM64T) and future update kernels.

HPE QLogic FastLinQ 10/25/50 GbE Drivers for Red Hat Enterprise Linux 6 x86_64
Version: 8.33.17.0-1 **(Optional)**
Filename: kmod-qlgc-fastlinq-8.33.17.0-1.rhel6u8.x86_64.compsig; kmod-qlgc-fastlinq-8.33.17.0-1.rhel6u8.x86_64.rpm; kmod-qlgc-fastlinq-8.33.17.0-1.rhel6u9.x86_64.compsig; kmod-qlgc-fastlinq-8.33.17.0-1.rhel6u9.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE QLogic FastLinQ Online Firmware Upgrade Utility for Linux x86_64*, version 1.4.24 or later, for use with these drivers.

Fixes

This product corrects a system crash seen when MFW calls for protocol stats while function is still probing.
This product corrects an issue seen when setting limits for LL2 buffer size.

Enhancements

This product now supports maximum transfer rate configuration for Packet Filters [packet pacing].
This product now supports Macvlan offload.
This product now supports 'link_change_count' in the port statistics.
This product now supports LL2 buffer or ping packet size settings by module param.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic FastLinQ 10/25/50 GbE Drivers for Red Hat Enterprise Linux 7 x86_64
Version: 8.33.17.0-1 **(Optional)**
Filename: kmod-qlgc-fastlinq-8.33.17.0-1.rhel7u4.x86_64.compsig; kmod-qlgc-fastlinq-8.33.17.0-1.rhel7u4.x86_64.rpm; kmod-qlgc-fastlinq-8.33.17.0-1.rhel7u5.x86_64.compsig; kmod-qlgc-fastlinq-8.33.17.0-1.rhel7u5.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE QLogic FastLinQ Online Firmware Upgrade Utility for Linux x86_64*, version 1.4.24 or later, for use with these drivers.

Fixes

This product corrects a system crash seen when MFW calls for protocol stats while function is still probing.
This product corrects an issue seen when setting limits for LL2 buffer size.

Enhancements

This product now supports maximum transfer rate configuration for Packet Filters [packet pacing].
This product now supports Macvlan offload.
This product now supports 'link_change_count' in the port statistics.
This product now supports LL2 buffer or ping packet size settings by module param.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic FastLinQ 10/25/50 GbE Drivers for SUSE Linux Enterprise Server 11 x86_64
Version: 8.33.17.0-1 **(Optional)**
Filename: qlgc-fastlinq-kmp-default-8.33.17.0_3.0.101_63-1.sles11sp4.x86_64.compsig; qlgc-fastlinq-kmp-default-8.33.17.0_3.0.101_63-1.sles11sp4.x86_64.rpm; qlgc-fastlinq-kmp-xen-8.33.17.0_3.0.101_63-1.sles11sp4.x86_64.compsig; qlgc-fastlinq-kmp-xen-8.33.17.0_3.0.101_63-1.sles11sp4.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE QLogic FastLinQ Online Firmware Upgrade Utility for Linux x86_64*, version 1.4.24 or later, for use with these drivers.

Fixes

This product corrects a system crash seen when MFW calls for protocol stats while function is still probing.
This product corrects an issue seen when setting limits for LL2 buffer size.

Enhancements

This product now supports maximum transfer rate configuration for Packet Filters [packet pacing].
This product now supports Macvlan offload.
This product now supports 'link_change_count' in the port statistics.
This product now supports LL2 buffer or ping packet size settings by module param.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic FastLinQ 10/25/50 GbE Drivers for SUSE Linux Enterprise Server 12 x86_64
Version: 8.33.17.0-1 **(Optional)**
Filename: qlgc-fastlinq-kmp-default-8.33.17.0_k4.4.21_69-1.sles12sp2.x86_64.compsig; qlgc-fastlinq-kmp-default-8.33.17.0_k4.4.21_69-1.sles12sp2.x86_64.rpm; qlgc-fastlinq-kmp-default-8.33.17.0_k4.4.73_5-1.sles12sp3.x86_64.compsig; qlgc-fastlinq-kmp-default-8.33.17.0_k4.4.73_5-1.sles12sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE QLogic FastLinQ Online Firmware Upgrade Utility for Linux x86_64*, version 1.4.24 or later, for use with these drivers.

Fixes

This product corrects a system crash seen when MFW calls for protocol stats while function is still probing.
This product corrects an issue seen when setting limits for LL2 buffer size.

Enhancements

This product now supports maximum transfer rate configuration for Packet Filters [packet pacing].
This product now supports Macvlan offload.
This product now supports 'link_change_count' in the port statistics.
This product now supports LL2 buffer or ping packet size settings by module param.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic FastLinQ 10/25/50 GbE Drivers for Windows Server x64 Editions
Version: 8.33.23.0 **(Optional)**
Filename: cp033844.compsig; cp033844.exe

Important Note!

HPE recommends the firmware provided in *HPE QLogic FastLinQ Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with these drivers.

Fixes

- This driver addresses an issue where iWARP does not appear under Device Manager advanced properties when in RDMA mode.
- This driver addresses an issue where the link speed is always shown to be 10Gbps.
- This driver addresses a system crash seen when changing NIC advanced parameters after running iWARP traffic.
- This driver addresses a system crash seen while loading or unloading the VBD driver with RoCE traffic.
- This driver addresses a system crash seen when the Virtual Switch RSS parameter is disabled.
- This driver addresses a system crash seen upon reboot while running traffic on virtual machine queues with a guest driver configured.
- This driver addresses a system crash seen when disabling IPv6 binding from adapter ports.
- This driver addresses a system crash seen when disabling a miniport with Driver Verifier.
- This driver corrects an issue where RSS processor selection across different NUMA nodes does not happen when the processor groups are different.
- This driver corrects an issue where unexpected L2 traffic is received.
- This driver corrects a mismatch in the maximum range for the iWARP Receive Window Size.
- This driver corrects an issue where host DCB settings don't take effect with an adapter in Non-Willing mode.

Enhancements

The maximum number of RDMA Queue Pairs (QPs) has been increased to 4096.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic FastLinQ 10/25/50 GbE Multifunction Driver for VMware vSphere 6.0
Version: 2018.06.04 **(Optional)**
Filename: cp033819.compsig; cp033819.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hp.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE QLogic FastLinQ Online Firmware Upgrade Utility for VMware*, version 4.6.24 or later, for use with this driver.

Fixes

This product resolves an issue where the system hangs during reboot.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic FastLinQ 10/25/50 GbE Multifunction Driver for VMware vSphere 6.5
Version: 2018.06.04 **(Optional)**
Filename: cp033820.compsig; cp033820.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hp.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE QLogic FastLinQ Online Firmware Upgrade Utility for VMware*, version 4.6.24 or later, for use with this driver.

Fixes

This product resolves an issue where the system hangs during reboot.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic FastLinQ RoCE Library for Red Hat Enterprise Linux 6 Update 8
Version: 8.33.1.0-1 **(Optional)**
Filename: qlgc-libqedr-8.33.1.0-1.rhel6u8.x86_64.compsig; qlgc-libqedr-8.33.1.0-1.rhel6u8.x86_64.rpm; README

Prerequisites

HPE QLogic FastLinQ 10/25/50GbE Drivers for Red Hat Enterprise Linux 6 x86_64, version 8.33.17.0-1 or later, must be installed before installing this product.

The libibverb package must be installed on the target system prior to the installation of the RoCE library. If not already present, the libibverb

package can be obtained from the operating system installation media.

Fixes

This product corrects a rstream application hang seen when using legacy Data Protection Manager (DPM).

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic FastLinQ RoCE Library for Red Hat Enterprise Linux 6 Update 9
Version: 8.33.1.0-1 **(Optional)**
Filename: qlgc-libqedr-8.33.1.0-1.rhel6u9.x86_64.compsig; qlgc-libqedr-8.33.1.0-1.rhel6u9.x86_64.rpm; README

Prerequisites

HPE QLogic FastLinQ 10/25/50GbE Drivers for Red Hat Enterprise Linux 6 x86_64, version 8.33.17.0-1 or later, must be installed before installing this product.

The libibverb package must be installed on the target system prior to the installation of the RoCE library. If not already present, the libibverb package can be obtained from the operating system installation media.

Fixes

This product corrects a rstream application hang seen when using legacy Data Protection Manager (DPM).

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic FastLinQ RoCE Library for SUSE Linux Enterprise Server 11 SP4
Version: 8.33.1.0-1 **(Optional)**
Filename: qlgc-libqedr-8.33.1.0-1.sles11sp4.x86_64.compsig; qlgc-libqedr-8.33.1.0-1.sles11sp4.x86_64.rpm; README

Prerequisites

HPE QLogic FastLinQ 10/25/50GbE Drivers for SUSE Linux Enterprise Server 11 x86_64, version 8.33.17.0-1 or later, must be installed before installing this product.

The libibverb package must be installed on the target system prior to the installation of the RoCE library. If not already present, the libibverb package can be obtained from the operating system installation media.

Fixes

This product corrects a rstream application hang seen when using legacy Data Protection Manager (DPM).

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic FastLinQ RoCE Library for SUSE Linux Enterprise Server 12 SP2
Version: 8.33.1.0-1 **(Optional)**
Filename: qlgc-libqedr-8.33.1.0-1.sles12sp2.x86_64.compsig; qlgc-libqedr-8.33.1.0-1.sles12sp2.x86_64.rpm; README

Prerequisites

HPE QLogic FastLinQ 10/25/50GbE Drivers for SUSE Linux Enterprise Server 12 x86_64, version 8.33.17.0-1 or later, must be installed before installing this product.

The libibverb package must be installed on the target system prior to the installation of the RoCE library. If not already present, the libibverb package can be obtained from the operating system installation media.

Fixes

This product corrects a rstream application hang seen when using legacy Data Protection Manager (DPM).

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic iSCSI Offload IO Daemon for Red Hat Enterprise Linux 6 Update 8 x86_64
Version: 2.11.5.5-6 **(Optional)**
Filename: iscsiuio-2.11.5.5-6.rhel6u8.x86_64.compsig; iscsiuio-2.11.5.5-6.rhel6u8.x86_64.rpm; README

Fixes

This product addresses an iSCSI BFS failure in DHCP seen when source and destination addresses are in different networks.
This product corrects a segmentation fault is seen when discovery is attempted on an unreachable target.

Enhancements

This product now supports the qedi iSCSI transport.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP FlexFabric 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic iSCSI Offload IO Daemon for Red Hat Enterprise Linux 6 Update 9 x86_64
Version: 2.11.5.5-6 **(Optional)**
Filename: iscsiuio-2.11.5.5-6.rhel6u9.x86_64.compsig; iscsiuio-2.11.5.5-6.rhel6u9.x86_64.rpm; README

Fixes

This product addresses an iSCSI BFS failure in DHCP seen when source and destination addresses are in different networks.
This product corrects a segmentation fault is seen when discovery is attempted on an unreachable target.

Enhancements

This product now supports the qedi iSCSI transport.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP FlexFabric 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic iSCSI Offload IO Daemon for Red Hat Enterprise Linux 7 Update 4 x86_64
Version: 2.11.5.5-6 **(Optional)**
Filename: iscsiuio-2.11.5.5-6.rhel7u4.x86_64.compsig; iscsiuio-2.11.5.5-6.rhel7u4.x86_64.rpm; README

Fixes

This product addresses an iSCSI BFS failure in DHCP seen when source and destination addresses are in different networks.
This product corrects a segmentation fault is seen when discovery is attempted on an unreachable target.

Enhancements

This product now supports the qedi iSCSI transport.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP FlexFabric 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic iSCSI Offload IO Daemon for Red Hat Enterprise Linux 7 Update 5 x86_64
Version: 2.11.5.5-6 **(Optional)**
Filename: iscsiuio-2.11.5.5-6.rhel7u5.x86_64.compsig; iscsiuio-2.11.5.5-6.rhel7u5.x86_64.rpm; README

Enhancements

Initial release.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP FlexFabric 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter

- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic iSCSI Offload IO Daemon for SUSE Linux Enterprise Server 11 SP3 x86_64
Version: 2.11.5.5-6 **(Optional)**
Filename: iscsiuio-2.11.5.5-6.sles11sp3.x86_64.compsig; iscsiuio-2.11.5.5-6.sles11sp3.x86_64.rpm; README

Fixes

This product addresses an iSCSI BFS failure in DHCP seen when source and destination addresses are in different networks.
This product corrects a segmentation fault is seen when discovery is attempted on an unreachable target.

Enhancements

This product now supports the qedi iSCSI transport.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP FlexFabric 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic iSCSI Offload IO Daemon for SUSE Linux Enterprise Server 11 SP4 x86_64
Version: 2.11.5.5-6 **(Optional)**
Filename: iscsiuio-2.11.5.5-6.sles11sp4.x86_64.compsig; iscsiuio-2.11.5.5-6.sles11sp4.x86_64.rpm; README

Fixes

This product addresses an iSCSI BFS failure in DHCP seen when source and destination addresses are in different networks.
This product corrects a segmentation fault is seen when discovery is attempted on an unreachable target.

Enhancements

This product now supports the qedi iSCSI transport.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP FlexFabric 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter

- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic iSCSI Offload IO Daemon for SUSE Linux Enterprise Server 12 SP2 x86_64
Version: 2.11.5.5-6 **(Optional)**
Filename: iscsiuio-2.11.5.5-6.sles12sp2.x86_64.compsig; iscsiuio-2.11.5.5-6.sles12sp2.x86_64.rpm; README

Fixes

This product addresses an iSCSI BFS failure in DHCP seen when source and destination addresses are in different networks.
This product corrects a segmentation fault is seen when discovery is attempted on an unreachable target.

Enhancements

This product now supports the qedi iSCSI transport.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP FlexFabric 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic iSCSI Offload IO Daemon for SUSE Linux Enterprise Server 12 SP3 x86_64
Version: 2.11.5.5-6 **(Optional)**
Filename: iscsiuio-2.11.5.5-6.sles12sp3.x86_64.compsig; iscsiuio-2.11.5.5-6.sles12sp3.x86_64.rpm; README

Fixes

This product addresses an iSCSI BFS failure in DHCP seen when source and destination addresses are in different networks.
This product corrects a segmentation fault is seen when discovery is attempted on an unreachable target.

Enhancements

This product now supports the qedi iSCSI transport.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP FlexFabric 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter

- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic NX2 10/20 GbE Multifunction Driver for VMware vSphere 6.0
Version: 2018.03.00 **(Recommended)**
Filename: cp035314.compsig; cp035314.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hp.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE QLogic NX2 Online Firmware Upgrade Utility for VMware*, version 1.20.14 or later, for use with this driver.

Fixes

This product addresses an issue where an 'HPE Synergy 3820C 10/20 Gb Converged Network Adapter' may crash when enabling SR-IOV (Single Root I/O Virtualization).

This product addresses an issue where the link status for an 'HPE Synergy 3820C 10/20Gb Converged Network Adapter' that is configured in a Link Aggregation Group (LAG) using 'HPE Virtual Connect SE 40Gb F8 Module for Synergy' may show as down at the Virtual Connect (VC) management console.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP NC532m Dual Port 10GbE Multifuntion BL-c Adapter
- HP Ethernet 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gb Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

HPE QLogic NX2 10/20 GbE Multifunction Driver for VMware vSphere 6.5
Version: 2018.06.04 **(Optional)**
Filename: cp033991.compsig; cp033991.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip file that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hp.com webpages, plus an HPE specific CP0xxxxx.xml file.

HPE recommends the firmware provided in *HPE QLogic NX2 Online Firmware Upgrade Utility for VMware*, version 1.21.15 or later, for use with this driver.

Fixes

- This product resolves an issue where the system hangs during reboot.
- This product addresses an issue where the FCoE link status is incorrect.
- This product resolves an Uncorrectable Machine Check Exception seen on shutdown.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter

- HP Ethernet 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 10Gb 2-port 2820C Converged Network Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

HPE QLogic NX2 10/20 GbE Multifunction Drivers for Red Hat Enterprise Linux 6 x86_64
Version: 7.14.46-1 **(Optional)**
Filename: kmod-netxtreme2-7.14.46-1.rhel6u8.x86_64.compsig; kmod-netxtreme2-7.14.46-1.rhel6u8.x86_64.rpm; kmod-netxtreme2-7.14.46-1.rhel6u9.x86_64.compsig; kmod-netxtreme2-7.14.46-1.rhel6u9.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE QLogic NX2 Online Firmware Upgrade Utility for Linux x86_64,* version 2.22.15 or later, for use with these drivers.

Fixes

This product corrects an error seen when creating a vlan interface in QinQ vlan mode.
This product corrects an issue seen when setting PVID priority in vlan mode.
This product corrects an error seen when getting traffic from a SR-IOV VM to a Virt-IO VM through the same physical function (PF).
This product corrects an error where a system crash occurs when reading cnic sfp data.
This product corrects an issue seen when updating the bnx2i driver.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP Ethernet 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

HPE QLogic NX2 10/20 GbE Multifunction Drivers for Red Hat Enterprise Linux 7 x86_64
Version: 7.14.46-1 **(Optional)**
Filename: kmod-netxtreme2-7.14.46-1.rhel7u4.x86_64.compsig; kmod-netxtreme2-7.14.46-1.rhel7u4.x86_64.rpm; kmod-netxtreme2-7.14.46-1.rhel7u5.x86_64.compsig; kmod-netxtreme2-7.14.46-1.rhel7u5.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE QLogic NX2 Online Firmware Upgrade Utility for Linux x86_64,* version 2.22.15 or later, for use with these drivers.

Fixes

This product corrects an error seen when creating a vlan interface in QinQ vlan mode.
This product corrects an issue seen when setting PVID priority in vlan mode.
This product corrects an error seen when getting traffic from a SR-IOV VM to a Virt-IO VM through the same physical function (PF).
This product corrects an error where a system crash occurs when reading cnic sfp data.
This product corrects an issue seen when updating the bnx2i driver.
This product corrects an issue seen when setting PVID for VFs in rhel7u4 using the ip tool.

Enhancements

This product now supports Red Hat Enterprise Linux 7.5.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP Ethernet 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

HPE QLogic NX2 10/20 GbE Multifunction Drivers for SUSE Linux Enterprise Server 11 x86_64
Version: 7.14.46-1 **(Optional)**
Filename: netxtreme2-kmp-default-7.14.46_3.0.101_63-1.sles11sp4.x86_64.compsig; netxtreme2-kmp-default-7.14.46_3.0.101_63-1.sles11sp4.x86_64.rpm; netxtreme2-kmp-default-7.14.46_3.0.76_0.11-1.sles11sp3.x86_64.compsig; netxtreme2-kmp-default-7.14.46_3.0.76_0.11-1.sles11sp3.x86_64.rpm; netxtreme2-kmp-xen-7.14.46_3.0.101_63-1.sles11sp4.x86_64.compsig; netxtreme2-kmp-xen-7.14.46_3.0.101_63-1.sles11sp4.x86_64.rpm; netxtreme2-kmp-xen-7.14.46_3.0.76_0.11-1.sles11sp3.x86_64.compsig; netxtreme2-kmp-xen-7.14.46_3.0.76_0.11-1.sles11sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE QLogic NX2 Online Firmware Upgrade Utility for Linux x86_64,* version 2.22.15 or later, for use with these drivers.

Fixes

This product corrects an error seen when creating a vlan interface in QinQ vlan mode.
This product corrects an issue seen when setting PVID priority in vlan mode.
This product corrects an error seen when getting traffic from a SR-IOV VM to a Virt-IO VM through the same physical function (PF).
This product corrects an error where a system crash occurs when reading cnic sfp data.
This product corrects an issue seen when updating the bnx2i driver.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP Ethernet 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

HPE QLogic NX2 10/20 GbE Multifunction Drivers for SUSE Linux Enterprise Server 12 x86_64
Version: 7.14.46-1 **(Optional)**
Filename: netxtreme2-kmp-default-7.14.46_k4.4.21_69-1.sles12sp2.x86_64.compsig; netxtreme2-kmp-default-7.14.46_k4.4.21_69-1.sles12sp2.x86_64.rpm; netxtreme2-kmp-default-7.14.46_k4.4.73_5-1.sles12sp3.x86_64.compsig; netxtreme2-kmp-default-7.14.46_k4.4.73_5-1.sles12sp3.x86_64.rpm; README

Important Note!

HPE recommends the firmware provided in *HPE QLogic NX2 Online Firmware Upgrade Utility for Linux x86_64,* version 2.22.15 or later, for use with these drivers.

Fixes

This product corrects an error seen when creating a vlan interface in QinQ vlan mode.
This product corrects an issue seen when setting PVID priority in vlan mode.
This product corrects an error seen when getting traffic from a SR-IOV VM to a Virt-IO VM through the same physical function (PF).
This product corrects an error where a system crash occurs when reading cnic sfp data.
This product corrects an issue seen when updating the bnx2i driver.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP Ethernet 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

HPE QLogic NX2 10/20 GbE Multifunction Drivers for Windows Server x64 Editions
Version: 7.13.145.0 **(Optional)**
Filename: cp034362.compsig; cp034362.exe

Important Note!

HP recommends the firmware provided in *HPE QLogic NX2 Online Firmware Upgrade Utility for Windows Server x64 Editions*, version 5.1.3.0 or later, for use with these drivers.

Fixes

This driver corrects an issue which results in a "MissingPFDriver" message appearing in Get-NetAdapterSriov command output.

Supported Devices and Features

This driver supports the following network adapters:

- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP Ethernet 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 10Gb 2820C Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

---

net-mst kernel module driver component for VMware 6.0
Version: 2018.01.22 **(Recommended)**
Filename: cp034694.compsig; cp034694.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HP applications. It is a zip that contains the same driver deliverable available from the HP vibsdepot.hp.com webpage, plus an HP specific CPXXXX.xml file.

Prerequisites

NA

Fixes

NMST version 4.9.0.38

Enhancements

NMST Version 4.9.0.38

---

net-mst kernel module driver component for VMware 6.5
Version: 2018.01.22 **(Recommended)**

Filename: cp034695.compsig; cp034695.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HP applications. It is a zip that contains the same driver deliverable available from the HP vibsdepot.hp.com webpage, plus an HP specific CPXXXX.xml file.

Prerequisites

NA

Fixes

NMST version 4.9.0.38

Enhancements

NMST Version 4.9.0.38

---

nmlx4_en driver component for VMware 6.0
Version: 2018.03.13 **(Recommended)**
Filename: cp035374.zip; cp035374_part1.compsig; cp035374_part2.compsig
Driver Name and Version:

Important Note!

Known Issues:

- PFC related priority counters are always set to 0, even if the PFC mode is enabled.
- The command "esxcli network sriovnic vf stats" is not supported.
- ConnectX-3 Pro 10G adapter cards incorrectly report support for 40G speed when running the "esxcli network nic get" command.
- When the port is DOWN, the management interface "port type" field indicates one of the port types supported by the device, in the following order: TP, FIBER, DA, NONE. If the port supports several cable types, the first type in the list mentioned above will be printed.
- Managment interface port type field reports SFP-to-RJ45 cable as FIBER.
- Management interface auto negotiation field is equivalent to "esxcli network nic get -n vmnicX" field "Pause Autonegotiate".

Fixes

The following issues have been fixed in version 3.15.11.6 included in this driver smart component:

- Internal multicast loopback issue that broke LACP bonding protocol.

---

nmlx4_en driver component for VMware 6.5
Version: 2018.03.13 **(Recommended)**
Filename: cp035375.zip; cp035375_part1.compsig; cp035375_part2.compsig; cp035375_part3.compsig
Driver Name and Version:

Important Note!

Known Issues:

- PFC related priority counters are always set to 0, even if the PFC mode is enabled.
- The command "esxcli network sriovnic vf stats" is not supported.
- ConnectX-3 Pro 10G adapter cards incorrectly report support for 40G speed when running the "esxcli network nic get" command.
- When the port is DOWN, the management interface "port type" field indicates one of the port types supported by the device, in the following order: TP, FIBER, DA, NONE. If the port supports several cable types, the first type in the list mentioned above will be printed.
- Managment interface port type field reports SFP-to-RJ45 cable as FIBER.
- Management interface auto negotiation field is equivalent to "esxcli network nic get -n vmnicX" field "Pause Autonegotiate".

Enhancements

Changes and New Features in driver version 3.16.11.6 included in this Smart Component:

- Updated Management Interface APIs.

Added support for the following features:

- VXLAN hardware offload. VXLAN hardware offload enables the traditional offloads to be performed on the encapsulated traffic. With ConnectX®-3 Pro, data center operators can decouple the overlay network layer from the physical NIC performance, thus achieving native performance in the new network architecture.
- Packet Capture Utility: This utility duplicates all traffic, including RDMA, in its raw Ethernet form (before stripping) to a dedicated "sniffing" QP, and then passes it to an ESX drop capture point.
- Large Send Offload (TCP Segmentation Offload)
- Wake-On-LAN (only on supported hardware)
- Receive Side Scaling (RSS) Queues
- Multiple Tx/Rx rings
- NetQueue support
- Fixed Pass-Through
- MSI-X

---

nmlx5_en driver component for VMware ESXi 6.0
Version: 2018.01.22 **(Recommended)**
Filename: cp034603.compsig; cp034603.zip
Driver Name and Version:

Important Note!

Known Issues:

- On rare occasions, a Purple Screen of Death (PSOD) may occur when changing MTU during traffic.
- The maximum value of RSS must be lower than the number of CPU cores.
- The hardware can offload only up to 256B of headers.
- The "esxcli network sriovnic vf stats" command is not supported. When running this command on a vmknic, a failure message is displayed.
- Traffic cannot be sent between PV and SR-IOV Virtual Functions connected to different ports on the same HCA.
- Setting the "Allow Guest MTU Change" option in vSphere Client is currently not functional. Although guest MTU changes in SR-IOV are allowed, they do not affect the port's MTU and the guest's MTU remains the same as the PF MTU.
- Although 'drss' and 'rss' parameters are disabled by default, the displayed default values of drss/drss is "4" when querying the nmlx5_core module parameter.
- VST mode ConnectX-5 SR-IOV is currently not functional.
- While running "stress ipv6 all2all traffic", the MTU is changed several times and PSOD is excepted.
- When a guest is assigned an IB PCI passthru device or an IB VF, VMware Tools networking information for the guest may be incorrect. This affects how the guest networking information, such as interfaces and their IPs are displayed in vCenter.
- Operations on vmnics which are in passthrough mode are not supported.
- The 'esxcli mellanox uplink link info -u <vmnic_name>' command reports the 'Auto negotiation' capability always as 'true'.
- SMP MADs (ibnetdiscover, sminfo, iblinkinfo, smpdump, ibqueryerr, ibdiagnet and smpquery) are not supported on the VFs.
- Multicast and IPv6 traffic might be unstable over SR-IOV.
- Reboot is required after any SR-IOV configuration change.
- Firmware VF configuration must be N+1 (while N is the required VF number). For example: If your configuration requires 10 VFs, the firmware must be set to support 16 VFs (ESXi Limitation).
- Wake-on-LAN does not notify when invalid parameters are provided.
- Nested ESXi might not function properly.
- Device RSS fails to hash traffic to sufficient RX rings with Broadcast traffic.
- In stress condition 'Watchdog' may appear, leading to uplink going up and down.
- Call trace might occur after running VGT with heavy traffic.
- VMs can get Call Trace upon MTU change during heavy traffic.
- Reloading the driver when the SR-IOV VFs are ON, will result in Purple Screen of Death (PSOD).
- VGT traffic over VXLAN interfaces is currently not supported.
- The adapter card might get stuck in Down state after setting the ring size to 8192.
- VMs with SR-IOV cannot be powered on when running low on available vectors.
- Occasionally, untagged traffic can pass between VMs with SR-IOV enabled when portgroup is configured for VLAN trunk range.

Fixes

The following issues have been fixed in driver version 4.15.13.2 included in this Smart Component:

- Disabled multicast loopback to avoid a scenario that prevented MAC learning in some configurations.
- Encapsulated traffic (VXLAN/Geneve) directed to NetQ RSS queue was not distributed through all queues' channels, thus did not utilize the RSS feature.

---

nmlx5_en driver component for VMware ESXi 6.5
Version: 2018.01.22 **(Recommended)**
Filename: cp034604.zip; cp034604_part1.compsig; cp034604_part2.compsig
Driver Name and Version:

Important Note!

Known Issues in version 4.16.12.12:

- The maximum value of RSS must be lower than the number of CPU cores.
- The hardware can offload only up to 256 Bytes of headers.
- The "esxcli network sriovnic vf stats" command is not supported.
- Traffic cannot be sent between PV and SR-IOV VF connected to different ports on the same HCA.
- Setting the "Allow Guest MTU Change" option in vSphere Client is currently not functional. Although guest MTU changes in SR-IOV are allowed, they do not affect the port's MTU and the guest's MTU remains the same as the PF MTU.
- VST mode in ConnectX-5 SR-IOV is currently not functional.
- Geneve options length support is limited to 56 Bytes. Received packets with options length bigger than 56 Bytes are dropped.
- Interaction with ConnectX-4/ConnectX-4 Lx older firmware versions might result in the following internal firmware errors:
- Device health compromised
- synd 0x1: firmware internal error
- extSync 0x94ee
- Operations on vmnics in passthrough mode are not supported.
- The 'esxcli mellanox uplink link info -u <vmnic_name>' command reports the 'Auto negotiation' capability always as 'true'.
- Multicast and IPv6 traffic might be unstable over SR-IOV.
- Reboot is required after any SR-IOV configuration change.
- Firmware VF configuration must be N+1 (while N is the required VF number). For example: If your configuration requires 10 VFs, the firmware must be set to support 16 VFs (ESXi Limitation).
- Wake-on-LAN does not notify when invalid parameters are provided.
- Nested ESXi might not function properly.
- Device RSS fails to hash traffic to sufficient RX rings with Broadcast traffic.
- In stress condition 'Watchdog' may appear leading to link going up and down.
- VMs can get Call Trace upon MTU change during heavy traffic.
- Reloading the driver when the SR-IOV VFs are ON, will result in Purple Screen of Death (PSOD).
- VGT traffic over VXLAN interfaces is currently not supported.
- VMs with SR-IOV cannot be powered on when running low on available vectors.
- Occasionally, untagged traffic can pass between VMs with SR-IOV enabled when portgroup is configured for VLAN trunk range.

Fixes

The following issues have been fixed in version 4.16.12.12:

- Encapsulated traffic (VXLAN/Geneve) directed to NetQ RSS queue was not distributed through all queues' channels, thus did not utilize the RSS feature.

Enhancements

New features and changes in version 4.16.12.12:

- Added support for Packet Capture Utility: This utility duplicates all traffic, including RDMA, in its raw Ethernet form (before stripping) to a dedicated "sniffing" QP, and then passes it to an ESX drop capture point.
- Changed the type of the SR-IOV max_vfs module parameter from a single integer value to an array of unsigned integers.

VMware ESX 6.0 MST Drivers Offline Bundle for Mellanox Adapters
Version: 4.9.0.38 **(Recommended)**
Filename: MLNX-NMST-ESX-6.0.0-4.9.0.38.zip

Prerequisites

NA

Enhancements

VM60 nmst 4.9.0.38

VMware ESX 6.5 MST Drivers Offline Bundle for Mellanox Adapters
Version: 4.9.0.38 **(Recommended)**
Filename: MLNX-NMST-ESX-6.5.0-4.9.0.38.zip

Prerequisites

NA

Enhancements

VM65 nmst 4.9.0.38

Driver - Security Top

AMD Secure Processor Driver for Windows Server 2012 R2
Version: 4.1.0.0 (C) **(Optional)**
Filename: cp034066.compsig; cp034066.exe

Enhancements

Added support for the HPE ProLiant DL325 Gen10.

AMD Secure Processor Driver for Windows Server 2016
Version: 4.1.0.0 (C) **(Optional)**
Filename: cp034067.compsig; cp034067.exe

Enhancements

Added support for the HPE ProLiant DL325 Gen10.

Driver - Storage Top

Dynamic Smart Array B140i Controller Driver for 64-bit Microsoft Windows Server 2012/2016 Editions
Version: 62.12.0.64 **(Recommended)**
Filename: cp028631.exe

Fixes

Blue Screen of Death (BSOD) displayed after installing Microsoft Windows Server 2012 R2 on systems configured with a HPE Dynamic Smart Array B140i RAID Controller and CPU count higher than the driver anticipated supporting (typically more than 128 CPU cores).

When running "Hypervisor Code Integrity Readiness Test", the WHQL test would fail.

Enhancements

Reduce debug output from optical devices to filter out unwanted messages and retain only the critical data.

Added support for Microsoft Windows Server 2016.

HPE Smart Array S100i SR Gen10 SW RAID Driver for Windows Server 2012 R2 and Windows Server 2016
Version: 62.2.20.64 (A) **(Recommended)**
Filename: cp035068.compsig; cp035068.exe

Important Note!

- Customers who already have firmware version 62.2.20.64 installed do not need to update to 62.2.20.64(A).

Enhancements

Added HPE Digital Signature

Driver - Storage Controller Top

HPE Dynamic Smart Array B140i Controller Driver for VMware vSphere 6.0 (Driver Component).
Version: 2017.09.25 **(Recommended)**
Filename: cp032629.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Fixes

Fixes an issue with the physical memory above 1TB where the driver could potentially create excessive error messages in vmkernel.log.

HPE Dynamic Smart Array B140i Controller Driver for VMware vSphere 6.5 (Driver Component).
Version: 2017.09.25 **(Recommended)**
Filename: cp032630.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the

vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Fixes

Fixes an issue with the physical memory above 1TB where the driver could potentially create excessive error messages in vmkernel.log.

HPE Dynamic Smart Array B140i SATA RAID Controller Driver for Red Hat Enterprise Linux 6 (64-bit)
Version: 1.2.10-120 **(Recommended)**
Filename: kmod-hpdsa-1.2.10-120.rhel6u8.x86_64.rpm; kmod-hpdsa-1.2.10-120.rhel6u9.x86_64.rpm

Fixes

The following issue has been resolved:

In a system configured with the HPE Dynamic Smart Array B140i Controller and higher than 128 CPU (cores), a system failure event would occur.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 6 (64-bit) supported by this binary rpm are:
2.6.32-642.el6 - Red Hat Enterprise Linux 6 Update 8(64-bit) and future errata kernels for update 8.
2.6.32-696.el6 - Red Hat Enterprise Linux 6 Update 9(64-bit) and future errata kernels for update 9.

HPE Dynamic Smart Array B140i SATA RAID Controller Driver for Red Hat Enterprise Linux 7 (64-bit)
Version: 1.2.10-137 (A) **(Recommended)**
Filename: kmod-hpdsa-1.2.10-137.rhel7u4.x86_64.rpm; kmod-hpdsa-1.2.10-137.rhel7u5.x86_64.rpm

Enhancements

- Added support for Red Hat Enterprise Linux 7.4.

Note: If driver version 1.2.10-137 was previously installed, then it is not necessary to upgrade to version 1.2.10-137(A).

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 7 (64-bit) supported by this binary rpm are:
3.10.0-693.el7- Red Hat Enterprise Linux 7 Update 4 (64-bit) and future errata kernels for update 4.
3.10.0-862.el7- Red Hat Enterprise Linux 7 Update 5 (64-bit) and future errata kernels for update 5.

HPE Dynamic Smart Array B140i SATA RAID Controller Driver for SUSE LINUX Enterprise Server 11 (64-bit)
Version: 1.2.10-120 **(Recommended)**
Filename: hpdsa-kmp-default-1.2.10-120.sles11sp3.x86_64.rpm; hpdsa-kmp-default-1.2.10-120.sles11sp4.x86_64.rpm; hpdsa-kmp-xen-1.2.10-120.sles11sp3.x86_64.rpm; hpdsa-kmp-xen-1.2.10-120.sles11sp4.x86_64.rpm

Fixes

The following issue has been resolved:

In a system configured with the HPE Dynamic Smart Array B140i Controller and higher than 128 CPU (cores), a system failure event would occur.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 11 (64-bit) supported by this binary rpm are:
3.0.76-0.11.1 - SUSE LINUX Enterprise Server 11 SP 3 (64-bit) and future errata kernels for SP 3.
3.0.101-63-default - SUSE LINUX Enterprise Server 11 SP 4 (64-bit) and future errata kernels for SP 4.

HPE Dynamic Smart Array B140i SATA RAID Controller Driver for SUSE LINUX Enterprise Server 12 (64-bit)
Version: 1.2.10-135 **(Recommended)**
Filename: hpdsa-kmp-default-1.2.10-135.sles12sp2.x86_64.rpm; hpdsa-kmp-default-1.2.10-135.sles12sp3.x86_64.rpm

Fixes

Controller Could stop responding after upgrading OS with a newer kernel version

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 12 (64-bit) supported by this binary rpm are:
4.4.21-69-default - SUSE LINUX Enterprise Server 12 (64-bit) SP2 plus future errata.
4.4.73-5.1 - SUSE LINUX Enterprise Server 12 (64-bit) SP3 plus future errata.

HPE Dynamic Smart Array Controller Driver for VMware vSphere 6.0 (Bundle file).
Version: 5.5.0.60-1 **(Recommended)**
Filename: hpdsa-5.5.0.60.zip

Fixes

Fixes an issue with the physical memory above 1TB where the driver could potentially create excessive error messages in vmkernel.log.

HPE Dynamic Smart Array Controller Driver for VMware vSphere 6.5 (Bundle file).
Version: 5.5.0.60-1 **(Recommended)**
Filename: hpdsa-5.5.0.60.zip

Fixes

Fixes an issue with the physical memory above 1TB where the driver could potentially create excessive error messages in vmkernel.log.

HPE H2xx SAS/SATA Host Bus Adapter (64-bit) Driver for vSphere 6.0 (Driver Component).
Version: 2016.03.21 (A) **(Optional)**
Filename: cp031478.compsig; cp031478.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Fixes

Change implemented in version 2016.03.21(A):

- Changed versioning control for component deployment. Updated
- to support Service Pack for ProLiant version 2017.07.0.
  Note: If component version 2016.03.21 was previously installed, then it is not necessary to upgrade to version 2016.03.21(A).

Issues resolved in version 2016.03.21:

- None

Enhancements

Change implemented in version 2016.03.21(A):

- Updated to support Service Pack for ProLiant version 2017.07.0.
  Note: If component version 2016.03.21 was previously installed, then it is not necessary to upgrade to version 2016.03.21(A).

Enhancements/New Features implemented in version 2016.03.21:

- Added support for VMWare ESXi 6.0 Update 1

Supported Devices and Features

NOTE: HPE H221 Host Bus Adapter does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

HPE H2xx SAS/SATA Host Bus Adapter (64-bit) Driver for vSphere 6.5
Version: 15.10.07.00-1 (A) **(Optional)**
Filename: mpt2sas-15.10.07.00-esxi5.5-4778920.zip

Fixes

Change implemented in version 15.10.07.00-1(A):

- Updated to support Service Pack for ProLiant version 2017.07.0.
  Note: If driver version 15.10.07.00-1 was previously installed, then it is not necessary to upgrade to version 15.10.07.00-1(A).

Issues resolved in version 15.10.07.00-1:

- Fixes minor installation issue with the driver on VMware vSphere 6.5.

Supported Devices and Features

NOTE: HPE H221 Host Bus Adapter does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

HPE H2xx SAS/SATA Host Bus Adapter (64-bit) Driver for vSphere 6.5 (Driver Component).
Version: 2017.01.20 (A) **(Optional)**
Filename: cp032277.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Fixes

Change implemented in version 2017.01.20(A):

- Updated to support Service Pack for ProLiant version 2017.07.0.
  Note: If component version 2017.01.20 was previously installed, then it is not necessary to upgrade to version 2017.01.20(A).

Issues resolved in version 2017.01.20:

- Fixes minor installation issue with the driver on VMware vSphere 6.5.

Supported Devices and Features

NOTE: HPE H221 Host Bus Adapter does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

HPE H2xx SAS/SATA Host Bus Adapter Driver for 64-bit Microsoft Windows Server 2016 Editions
Version: 2.68.64.2 (B) **(Optional)**
Filename: cp032270.exe

Important Note!

This driver component supports Gen9 servers only with H221 controllers and the controller does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

Enhancements

Change implemented in version 2.68.64.2(B):

- Updated to support Service Pack for ProLiant version 2017.07.0.
  Note: If component version 2.68.64.2(A) was previously installed, then it is not necessary to upgrade to version 2.68.64.2(B).

Enhancements/New Features implemented in version 2.68.64.2(A):

Added support for:

- Microsoft Windows Server 2016 - Server Core and Server with a Desktop.
- Revised component package. No change to driver functionality resulting from the change. If system has previously updated to driver version 2.68.64.2, then it is not necessary to update to 2.68.64.2(A).

Supported Devices and Features

This driver component supports Gen9 servers only with H221 controllers and the controller does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers

---

HPE H2xx SAS/SATA Host Bus Adapter Driver for Microsoft Windows Server 2012 64-bit Editions
Version: 2.68.64.0 (B) **(Recommended)**

Filename: cp032610.exe

Enhancements

Change implemented in version 2.68.64.0(B):

- Updated to support Service Pack for ProLiant version 2.017.07.0.
  Note: If driver version 2.68.64.0 was previously installed, then it is not necessary to upgrade to version 2.68.64.0 (B).

Enhancements/New Features implemented in version 2.68.64.0:

- Updated for Version Control across all LSI_sas2 Windows Drivers.

Supported Devices and Features

This driver component supports Gen9 servers only with H221 controllers and the controller does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

HPE H2xx SAS/SATA Host Bus Adapter Driver for Microsoft Windows Server 2012 R2 64-bit Editions
Version: 2.68.64.1 (B) **(Optional)**
Filename: cp032453.exe

Enhancements

Change implemented in version 2.68.64.1(B):

- Updated to support Service Pack for ProLiant version 2017.07.0.
  Note: If driver version 2.68.64.1 was previously installed, then it is not necessary to upgrade to version 2.68.64.1(B).

Enhancements/New Features implemented in version 2.68.64.1:

- Added support for Windows 8.1 and Windows Server 2012R2 to the build scripts.
- Add build support for new Windows Event Logging.
- Add support for automatic selection of the default driver build parameters file during the build

Supported Devices and Features

This driver component supports Gen9 servers only with H221 controllers and the controller does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

HPE H2xx SAS/SATA Host Bus Adapter Driver for Red Hat Enterprise Linux 6 (64-bit)
Version: 15.10.05.00-6 **(Recommended)**
Filename: kmod-mpt2sas-15.10.04.00-10.rhel6u8.x86_64.rpm; kmod-mpt2sas-15.10.05.00-6.rhel6u9.x86_64.rpm

Enhancements

Added support for Red Hat Enterprise Linux 6 Update 9.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 6 (64-bit) supported by this binary rpm are:
2.6.32-642.el6 - Red Hat Enterprise Linux 6 Update 8(64-bit) and future errata kernels for update 8.
2.6.32-696.el6 - Red Hat Enterprise Linux 6 Update 9(64-bit) and future errata kernels for update 9.

NOTE: HPE H221 Host Bus Adapter does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

HPE H2xx SAS/SATA Host Bus Adapter Driver for Red Hat Enterprise Linux 7 (64-bit)
Version: 15.10.07.00-3 **(Recommended)**
Filename: kmod-mpt2sas-15.10.07.00-3.rhel7u5.x86_64.rpm

Enhancements

Added support for RHEL 7.5

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 7 (64-bit) supported by this binary rpm are:

- Red Hat Enterprise Linux 7 Update 4 (64-bit) and future errata kernels for update 5.

Note: This driver component supports Gen9 servers only with H221 controllers and the controller does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

HPE H2xx SAS/SATA Host Bus Adapter Driver for SUSE LINUX Enterprise Server 11 (64-bit)
Version: 15.10.04.00-5 (B) **(Recommended)**
Filename: lsi-mpt2sas-kmp-default-15.10.02.00-6.sles11sp3.x86_64.rpm; lsi-mpt2sas-kmp-default-15.10.04.00-5.sles11sp4.x86_64.rpm; lsi-mpt2sas-kmp-xen-15.10.02.00-6.sles11sp3.x86_64.rpm; lsi-mpt2sas-kmp-xen-15.10.04.00-5.sles11sp4.x86_64.rpm

Enhancements

Change implemented in version 15.10.04.00-5(B):

- Updated to support Service Pack for ProLiant version 2017.07.0.
  Note: If driver version 15.10.04.00-5(A) was previously installed, then it is not necessary to upgrade to version 15.10.04.00-5(B).

Enhancements/New Features implemented in version 15.10.04.00-5(A):

- Added HPE digital signatures to RPM packages and included kernel objects. No functional changes were made to the driver. If driver version 15.10.04.00-5 is installed on the target system, then it is not necessary to update to driver version 15.10.04.00-5(A).

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 11 (64-bit) supported by this driver diskette are:
3.0.76-0.11.1 - SUSE LINUX Enterprise Server 11 SP 3 (64-bit) plus future errata.
3.0.101-63-default - SUSE LINUX Enterprise Server 11 SP 4 (64-bit) plus future errata.

Note: This driver component supports Gen9 servers only with H221 controllers and the controller does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

HPE H2xx SAS/SATA Host Bus Adapter Driver for SUSE LINUX Enterprise Server 12 (64-bit)
Version: 15.10.06.00-6 **(Recommended)**
Filename: lsi-mpt2sas-kmp-default-15.10.06.00-2.sles12sp2.x86_64.rpm; lsi-mpt2sas-kmp-default-15.10.06.00-6.sles12sp3.x86_64.rpm

Enhancements

Added support for SUSE LINUX Enterprise Server 12 SP2 and SP3.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 12 (64-bit) supported by this binary rpm are:
4.4.21-69-default - SUSE LINUX Enterprise Server 12 (64-bit) SP2 plus future errata.
4.4.73-5.1 -SUSE LINUX Enterprise Server 12 (64-bit) SP3 plus future errata.

Note: This driver component supports Gen9 servers only with H221 controllers and the controller does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

HPE ProLiant Gen10 Smart Array Controller (64-bit) Driver for Red Hat Enterprise Linux 6 (64-bit)
Version: 1.1.4-125 **(Recommended)**
Filename: kmod-smartpqi-1.1.4-125.rhel6u9.x86_64.compsig; kmod-smartpqi-1.1.4-125.rhel6u9.x86_64.rpm

Fixes

- In rare cases, the driver might stop responding when using NCQ SATA drives.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 6 (64-bit) supported by this driver rpm are:
2.6.32-696.el6 - Red Hat Enterprise Linux 6 Update 9(64-bit) and future errata kernels for update 9.

Version: 1.1.4-125 (A) **(Recommended)**
Filename: kmod-smartpqi-1.1.4-125.rhel7u4.x86_64.compsig; kmod-smartpqi-1.1.4-125.rhel7u4.x86_64.rpm; kmod-smartpqi-1.1.4-125.rhel7u5.x86_64.compsig; kmod-smartpqi-1.1.4-125.rhel7u5.x86_64.rpm

Fixes

- In rare cases, the driver might stop responding when using NCQ SATA drives.

Enhancements

- Added support for Red Hat Enterprise Linux 7.4.

Note: If driver version 1.1.4-125 was previously installed, then it is not necessary to upgrade to version 1.1.4-125(A).

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux7 (64-bit) supported by this binary rpm are:
3.10.0-693.el7- Red Hat Enterprise Linux 7 Update 4 (64-bit) and future errata kernels for update 4.
3.10.0-862.el7- Red Hat Enterprise Linux 7 Update 5 (64-bit) and future errata kernels for update 5.

HPE ProLiant Gen10 Smart Array Controller (64-bit) Driver for SUSE LINUX Enterprise Server 11 (64-bit)
Version: 1.1.4-125 **(Recommended)**
Filename: smartpqi-kmp-default-1.1.4-125.sles11sp4.x86_64.compsig; smartpqi-kmp-default-1.1.4-125.sles11sp4.x86_64.rpm; smartpqi-kmp-xen-1.1.4-125.sles11sp4.x86_64.compsig; smartpqi-kmp-xen-1.1.4-125.sles11sp4.x86_64.rpm

Fixes

- In rare cases, the driver might stop responding when using NCQ SATA drives.

Supported Devices and Features

The kernels of SUSE LINUX Enterprise Server 11 (64-bit) supported by this driver diskette are:
3.0.101-63-default - SUSE LINUX Enterprise Server 11 SP 4 (64-bit) and future errata kernels for SP 4.

HPE ProLiant Gen10 Smart Array Controller (64-bit) Driver for SUSE LINUX Enterprise Server 12 (64-bit)
Version: 1.1.4-125 **(Recommended)**
Filename: smartpqi-kmp-default-1.1.4-125.sles12sp2.x86_64.compsig; smartpqi-kmp-default-1.1.4-125.sles12sp2.x86_64.rpm; smartpqi-kmp-default-1.1.4-125.sles12sp3.x86_64.compsig; smartpqi-kmp-default-1.1.4-125.sles12sp3.x86_64.rpm

Fixes

- In rare cases, the driver might stop responding when using NCQ SATA drives.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 12 (64-bit) supported by this binary rpm are:
4.4.21-69-default - SUSE LINUX Enterprise Server 12 (64-bit) SP2 plus future errata.
4.4.73-5.1 - SUSE LINUX Enterprise Server 12 (64-bit) SP3 plus future errata.

HPE ProLiant Smart Array Controller (64-bit) Driver for Red Hat Enterprise Linux 6 (64-bit)
Version: 3.4.20-125 **(Recommended)**
Filename: kmod-hpsa-3.4.20-125.rhel6u8.x86_64.rpm; kmod-hpsa-3.4.20-125.rhel6u9.x86_64.rpm

Fixes

Fixes an issue where the system could panic after a kernel buffer message "Inquiry failed"

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 6 (64-bit) supported by this driver diskette are:

2.6.32-642.el6 - Red Hat Enterprise Linux 6 Update 8(64-bit) and future errata kernels for update 8.
2.6.32-696.el6 - Red Hat Enterprise Linux 6 Update 9(64-bit) and future errata kernels for update 9.

HPE ProLiant Smart Array Controller (64-bit) Driver for Red Hat Enterprise Linux 7 (64-bit)
Version: 3.4.20-136 (A) **(Recommended)**
Filename: kmod-hpsa-3.4.20-136.rhel7u4.x86_64.rpm; kmod-hpsa-3.4.20-136.rhel7u5.x86_64.rpm

Enhancements

- Added support for Red Hat Enterprise Linux 7.4.

Note: If driver version 3.4.20-136 was previously installed, then it is not necessary to upgrade to version 3.4.20-136(A).

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 7 (64-bit) supported by this binary rpm are:
3.10.0-693.el7- Red Hat Enterprise Linux 7 Update 4 (64-bit) and future errata kernels for update 4.
3.10.0-862.el7- Red Hat Enterprise Linux 7 Update 5 (64-bit) and future errata kernels for update 5.

HPE ProLiant Smart Array Controller (64-bit) Driver for SUSE LINUX Enterprise Server 11 (64-bit)
Version: 3.4.20-125 **(Recommended)**
Filename: hpsa-kmp-default-3.4.20-125.sles11sp3.x86_64.rpm; hpsa-kmp-default-3.4.20-125.sles11sp4.x86_64.rpm; hpsa-kmp-xen-3.4.20-125.sles11sp3.x86_64.rpm; hpsa-kmp-xen-3.4.20-125.sles11sp4.x86_64.rpm

Fixes

Fixes an issue where the system could panic after a kernel buffer message "Inquiry failed"

Supported Devices and Features

The kernels of SUSE LINUX Enterprise Server 11 (64-bit) supported by this driver diskette are:
3.0.76-0.11.1 - SUSE LINUX Enterprise Server 11 SP 3 (64-bit) and future errata kernels for SP 3.
3.0.101-63-default - SUSE LINUX Enterprise Server 11 SP 4 (64-bit) and future errata kernels for SP 4.

HPE ProLiant Smart Array Controller (64-bit) Driver for SUSE LINUX Enterprise Server 12 (64-bit)
Version: 3.4.20-125 **(Recommended)**
Filename: hpsa-kmp-default-3.4.20-125.sles12sp2.x86_64.rpm; hpsa-kmp-default-3.4.20-125.sles12sp3.x86_64.rpm

Fixes

Fixes an issue where the system could panic after a kernel buffer message "Inquiry failed"

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 12 (64-bit) supported by this binary rpm are:
4.4.21-69-default - SUSE LINUX Enterprise Server 12 (64-bit) SP2 plus future errata.
4.4.73-5.1 - SUSE LINUX Enterprise Server 12 (64-bit) SP3 plus future errata.

HPE ProLiant Smart Array Controller Driver for VMware vSphere 6.0 (Bundle file)
Version: 6.0.0.132-1 **(Recommended)**
Filename: hpsa-6.0.0.132-7216129.zip

Enhancements

Improved driver handling of late I/O request completions to reduce the possibility of PSOD event.

HPE ProLiant Smart Array Controller Driver for VMware vSphere 6.0 (Driver Component).
Version: 2018.02.12 **(Recommended)**
Filename: cp033361.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the

vmware.com and the HPE http://vibsdepot.hpe.com/ webpages, plus an HPE specific CPXXXX.xml file.

Enhancements

Improved driver handling of late I/O request completions to reduce the possibility of PSOD event.

HPE ProLiant Smart Array Controller Driver for VMware vSphere 6.5 (Bundle file)
Version: 2.0.30-1 **(Recommended)**
Filename: VMW-ESX-6.5.0-nhpsa-2.0.30-7870290.zip

Enhancements

- Added a module parameter to enable VMware VSAN mode

HPE ProLiant Smart Array Controller Driver for VMware vSphere 6.5 (Driver Component).
Version: 2018.06.04 **(Recommended)**
Filename: cp034542.compsig; cp034542.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Enhancements

- Added a module parameter to enable VMware VSAN mode

HPE ProLiant Smart Array HPCISSS3 Controller Driver for 64-bit Microsoft Windows Server 2012/2012 R2/2016 Editions
Version: 100.20.0.64 (A) **(Recommended)**
Filename: cp033990.exe

Enhancements

Added support for Microsoft Windows 10

HPE Smart Array Gen10 Controller Driver for Windows Server 2012 R2 and Windows Server 2016
Version: 100.62.0.64 **(Recommended)**
Filename: cp034601.compsig; cp034601.exe

Fixes

- Microsoft Windows Server 2016 fails cluster validation test.
- Windows "Removal Policy" incorrectly set to TRUE.

HPE Smart Array P824i-p MR 64-bit controller driver for Microsoft Windows 2012 R2 edition.
Version: 6.714.8.0 **(Recommended)**
Filename: cp032292.compsig; cp032292.exe

Fixes

Initial driver release for HPE Smart Array P Class MR Gen10 controllers.

HPE Smart Array P824i-p MR 64-bit controller driver for Microsoft Windows 2016 edition.
Version: 6.714.8.0 **(Recommended)**
Filename: cp032262.compsig; cp032262.exe

Fixes

Initial driver release for HPE Smart Array P Class MR Gen10 controllers.

HPE Smart Array P824i-p MR controller Driver for 64-bit Red Hat Enterprise Linux 6
Version: 07.702.09.00-11 **(Recommended)**
Filename: kmod-megaraid_sas-07.702.09.00-11.rhel6u9.x86_64.compsig; kmod-megaraid_sas-07.702.09.00-11.rhel6u9.x86_64.rpm

Fixes

Initial driver release for HPE Smart Array P Class MR Gen10 controllers.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 6 (64-bit) supported by this binary rpm are:

2.6.32-696.el6 - Red Hat Enterprise Linux 6 Update 9(64-bit) and future errata kernels for update 9.

HPE Smart Array P824i-p MR controller Driver for 64-bit Red Hat Enterprise Linux 7
Version: 07.702.09.00-11 **(Recommended)**
Filename: kmod-megaraid_sas-07.702.09.00-11.rhel7u3.x86_64.compsig; kmod-megaraid_sas-07.702.09.00-11.rhel7u3.x86_64.rpm; kmod-megaraid_sas-07.702.09.00-11.rhel7u4.x86_64.compsig; kmod-megaraid_sas-07.702.09.00-11.rhel7u4.x86_64.rpm

Fixes

Initial driver release for HPE Smart Array P Class MR Gen10 controllers.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of Red Hat Enterprise Linux 7 (64-bit) supported by this binary rpm are:
3.10.0-514.el7- Red Hat Enterprise Linux 7 Update 3 (64-bit) and future errata kernels for update 3.
3.10.0-693.el7 - Red Hat Enterprise Linux 7 Update 4 (64-bit) and future errata kernels for update 4.

HPE Smart Array P824i-p MR controller Driver for 64-bit SUSE LINUX Enterprise Server 11
Version: 07.702.09.00-11 **(Recommended)**
Filename: lsi-megaraid_sas-kmp-default-07.702.09.00-11.sles11sp4.x86_64.compsig; lsi-megaraid_sas-kmp-default-07.702.09.00-11.sles11sp4.x86_64.rpm; lsi-megaraid_sas-kmp-xen-07.702.09.00-11.sles11sp4.x86_64.compsig; lsi-megaraid_sas-kmp-xen-07.702.09.00-11.sles11sp4.x86_64.rpm

Fixes

Initial driver release for HPE Smart Array P Class MR Gen10 controllers.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 11 (64-bit) supported by this driver diskette are:
3.0.101-63-default - SUSE LINUX Enterprise Server 11 SP 4 (64-bit) plus future errata.

HPE Smart Array P824i-p MR controller Driver for 64-bit SUSE LINUX Enterprise Server 12
Version: 07.702.09.00-11 **(Recommended)**
Filename: lsi-megaraid_sas-kmp-default-07.702.09.00-11.sles12sp2.x86_64.compsig; lsi-megaraid_sas-kmp-default-07.702.09.00-11.sles12sp2.x86_64.rpm; lsi-megaraid_sas-kmp-default-07.702.09.00-11.sles12sp3.x86_64.compsig; lsi-megaraid_sas-kmp-default-07.702.09.00-11.sles12sp3.x86_64.rpm

Fixes

Initial driver release for HPE Smart Array P Class MR Gen10 controllers.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 12 (64-bit) supported by this binary rpm are:
4.4.21-69-default - SUSE LINUX Enterprise Server 12 (64-bit) SP2 plus future errata.
4.4.73-5.1 - SUSE LINUX Enterprise Server 12 (64-bit) SP3 plus future errata.

HPE Smart Array S100i SR Gen10 SW RAID Driver for SUSE LINUX Enterprise Server 12
Version: 1.1.2-155 **(Recommended)**
Filename: smartdq-kmp-default-1.1.2-155.sles12sp2.x86_64.compsig; smartdq-kmp-default-1.1.2-155.sles12sp2.x86_64.rpm; smartdq-kmp-default-1.1.2-155.sles12sp3.x86_64.compsig; smartdq-kmp-default-1.1.2-155.sles12sp3.x86_64.rpm

Fixes

ID fix for the Cannon Lake systems.

Supported Devices and Features

SUPPORTED KERNELS:
The kernels of SUSE LINUX Enterprise Server 12 (64-bit) supported by this binary rpm are:
4.4.21-69-default - SUSE LINUX Enterprise Server 12 (64-bit) SP2 plus future errata.
4.4.73-5.1 - SUSE LINUX Enterprise Server 12 (64-bit) SP3 plus future errata.

Driver - Storage Fibre Channel and Fibre Channel Over Ethernet Top

HPE Storage Fibre Channel Adapter Kit for the x64 Emulex Storport Driver for Windows 2012, Windows 2012R2 and Windows 2016
Version: 11.4.334.7 **(Recommended)**
Filename: cp034221.compsig; cp034221.exe

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Enhancements

Updated to driver version 11.4.334.7

Removed the raw driver file folder. The raw driver files can be obtained by extracting the Smart Component and then extracting the Emulex installer. Use this command:

elxdrvr-fc-version.exe /q2 extract=2

The extracted files are located:

C:\Users\Administrator\Documents\Emulex\Drivers\FC-version

Each kit folder has subsequent architecture folders with subsequent OS folders. For example,

C:\Users\Administrator\Documents\Emulex\Drivers\FC-version\x64\win2012

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA

- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

HPE Storage Fibre Channel Adapter Kit for the x64 QLogic Storport Driver for Windows Server 2012 and 2012 R2
Version: 9.2.8.20 **(Recommended)**
Filename: cp034232.compsig; cp034232.exe

Important Note!

Release Notes:
HPE StoreFabric QLogic Adapters Release Notes

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Fixes

This driver version resolves the following :

- Switch name server entry, Port Symbols are displayed with dots at the end
- Non-descriptive Device name in Windows
- Request_Driver_Plogi(Port Login) Retry Delay
- Unexpected behavior of FC(Fibre Channel) speed - When transfer sizes above 8MB(MegaByte) are attempted, performance drops to almost zero by making mixed mode (I/O Control Block type 6 and 7) default and used IOCB (I/O Control Block) type 6 when IO(Input Output) size > 128K (> 0x20 segments)

Enhancements

Updated the driver to version 9.2.8.20

Added support for the following:

- Added ABTS (Abort Sequence) handling for passthru (pass through) ELS (Extended Link Services) to prevent FW (firmware) resource leak
- Updated RISC(Reduced Instruction Set Computer) FW (Firmware) to version 8.07.00 for 8G Adapters
- Driver always responds to RDP (Read Diagnostic Parameter) with full payload (new version of FW (firmware) will split it into multiple frames if there is no login session)
- Added new DPORT (Destination Port) diagnostic API (Application Program Interface) interface to return detailed codes
- Removed Echo only restriction for ELS (Extended Link Services) pass through
- Added GFO (Get Fabric Object) and LUN (Logical Unit) level QoS (Quality of Service) support
- Added ELS (Extended Link Services) passthru (pass through) interface

Supported Devices and Features

This driver supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

HPE Storage Fibre Channel Adapter Kit for the x64 QLogic Storport Driver for Windows Server 2016
Version: 9.2.8.20 **(Recommended)**
Filename: cp034233.compsig; cp034233.exe

Important Note!

Release Notes:
HPE StoreFabric QLogic Adapters Release Notes

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Fixes

This driver version resolves the following :

- Switch name server entry, Port Symbols are displayed with dots at the end
- Non-descriptive Device name in Windows
- Request_Driver_Plogi(Port Login) Retry Delay
- Unexpected behavior of FC(Fibre Channel) speed - When transfer sizes above 8MB(MegaByte) are attempted, performance drops to almost zero by making mixed mode (I/O Control Block type 6 and 7) default and used IOCB (I/O Control Block) type 6 when IO(Input Output) size > 128K (> 0x20 segments)

Enhancements

Updated the driver to version 9.2.8.20

Added support for the following:

- Added ABTS (Abort Sequence) handling for passthru (pass through) ELS (Extended Link Services) to prevent FW (firmware) resource leak
- Updated RISC(Reduced Instruction Set Computer) FW (Firmware) to version 8.07.00 for 8G Adapters
- Driver always responds to RDP (Read Diagnostic Parameter) with full payload (new version of FW (firmware) will split it into multiple frames if there is no login session)
- Added new DPORT (Destination Port) diagnostic API (Application Program Interface) interface to return detailed codes
- Removed Echo only restriction for ELS (Extended Link Services) pass through
- Added GFO (Get Fabric Object) and LUN (Logical Unit) level QoS (Quality of Service) support
- Added ELS (Extended Link Services) passthru (pass through) interface

Supported Devices and Features

This driver supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

HPE Storage Fibre Channel Over Ethernet Adapter Kit for the x64 Emulex Storport Driver for Windows 2012, Windows 2012R2 and Windows 2016
Version: 12.0.1109.0 **(Recommended)**
Filename: cp034220.compsig; cp034220.exe

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Enhancements

Updated to driver version 12.0.1109.0

Removed the raw driver file folder. The raw driver files can be obtained by extracting the Smart Component and then extracting the Emulex installer. Use this command:

brcmdrvr-fcoe-version.exe /q2 extract=2

The extracted files are located:

C:\Users\Administrator\Documents\Broadcom\Drivers\FCoE-version

Each kit folder has subsequent architecture folders with subsequent OS folders. For example,

C:\Users\Administrator\Documents\Broadcom\Drivers\FCoE-version\x64\win2012

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HPE StoreFabric CN1200E-T Adapter

Red Hat Enterprise Linux 6 Server (x86-64) FC Driver Kit for HPE Qlogic and mezzanine Host Bus Adapters
Version: 8.08.00.07.06.0-k1 **(Recommended)**
Filename: kmod-qlgc-qla2xxx-8.08.00.07.06.0_k1-1.rhel6u8.x86_64.compsig; kmod-qlgc-qla2xxx-8.08.00.07.06.0_k1-1.rhel6u8.x86_64.rpm; kmod-qlgc-qla2xxx-8.08.00.07.06.0_k1-1.rhel6u9.x86_64.compsig; kmod-qlgc-qla2xxx-8.08.00.07.06.0_k1-1.rhel6u9.x86_64.rpm

Important Note!

Release Notes

HPE StoreFabric QLogic Adapters Release Notes

Note: The rpm base-name for the QLogic driver has been changed to "qlgc". Upgrades from the earlier "hpqlgc" driver are supported.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Fixes

This driver version resolves the following:

- Mask off Scope bits in retry delay.
- Track if INQ (Inquiry) was sent, and send INQ (Inquiry) to all LUNs (Logical Unit).
- Prevent re_login trigger from sending too many commands
- Prevent multiple active discovery commands per session
- Correction to non-existent fabric name.
- Remove RDP (Read Diagnostic Parameter) response size cropping for logged out port.
- Fix supported speed ranges in FDMI/RDP (Fabric Device Management Interface /Read Diagnostic Parameter).
- GPID (Get Node Identification) Data unexpected terminations.
- Re-login for N-port Handle in use.
- Re-login is being triggered too fast.
- Reported supported link speeds.
- Add correction to fc (Fibre Channel) host stats (Statistics).

Enhancements

Updated to version 8.08.00.07.06.0-k1

Added support for the following:

- Handle cases for limiting Read Diagnostic Parameter (RDP) response payload length.
- Add fabric priority QoS (Quality of Service) lun (Logical Unit) IOCB (I/O Control Block) mechanism.
- Implement CT (Common Transport) command GFO (Get Fabric Object)
- Retry switch command on timed out.
- Add short name for SFP (Small Form-Factor Pluggable) range auto detect.
- Add ability to auto detect SFP (Small Form-Factor Pluggable) type.
- Add support for fabric priority per target.
- Allow Storage Name Service (SNS) fabric login to be retried.
- Increase the login retry count to 30.

Supported Devices and Features

This driver supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

Red Hat Enterprise Linux 6 Server (x86-64) FCoE Driver Kit for HPE Emulex(BRCM) Converged Network Adapters(CNAs) and mezzanine Converged Network Adapters(CNAs)
Version: 12.0.1110.11 **(Recommended)**
Filename: kmod-brcmfcoe-12.0.1110.11-1.rhel6u8.x86_64.compsig; kmod-brcmfcoe-12.0.1110.11-1.rhel6u8.x86_64.rpm; kmod-brcmfcoe-12.0.1110.11-1.rhel6u9.x86_64.compsig; kmod-brcmfcoe-12.0.1110.11-1.rhel6u9.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and

cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to Driver version 12.0.1110.11

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HPE StoreFabric CN1200E-T Adapter

Red Hat Enterprise Linux 6 Server (x86-64) Fibre Channel Driver Kit for HPE Emulex Host Bus Adapters and mezzanine Host Bus Adapters
Version: 11.4.334.12 **(Recommended)**
Filename: kmod-elx-lpfc-11.4.334.12-1.rhel6u8.x86_64.compsig; kmod-elx-lpfc-11.4.334.12-1.rhel6u8.x86_64.rpm; kmod-elx-lpfc-11.4.334.12-1.rhel6u9.x86_64.compsig; kmod-elx-lpfc-11.4.334.12-1.rhel6u9.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to driver version 11.4.334.12

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

Red Hat Enterprise Linux 7 Server FC Driver Kit for HPE QLogic and mezzanine Host Bus Adapters
Version: 8.08.00.07.07.5-k1 **(Recommended)**
Filename: kmod-qlgc-qla2xxx-8.08.00.07.07.0_k1-1.rhel7u4.x86_64.compsig; kmod-qlgc-qla2xxx-8.08.00.07.07.0_k1-1.rhel7u4.x86_64.rpm; kmod-qlgc-qla2xxx-8.08.00.07.07.5_k1-1.rhel7u5.x86_64.compsig; kmod-qlgc-qla2xxx-8.08.00.07.07.5_k1-1.rhel7u5.x86_64.rpm

Important Note!

Release Notes:

HPE StoreFabric QLogic Adapters Release Notes

Note: The rpm base-name for the QLogic driver has been changed to "qlgc". Upgrades from the earlier "hpqlgc" driver are supported.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Fixes

This driver version resolves the following:

- Mask off Scope bits in retry delay.
- Track if INQ (Inquiry) was sent, and send INQ (Inquiry) to all LUNs (Logical Unit).
- Prevent re_login trigger from sending too many commands
- Prevent multiple active discovery commands per session
- Correction to non-existent fabric name.
- Remove RDP (Read Diagnostic Parameter) response size cropping for logged out port.
- Fix supported speed ranges in FDMI/RDP (Fabric Device Management Interface /Read Diagnostic Parameter).
- GPID (Get Node Identification) Data unexpected terminations.
- Re-login for N-port Handle in use.
- Re-login is being triggered too fast.
- Reported supported link speeds.

- Add correction to fc (Fibre Channel) host stats (Statistics).

Enhancements

Updated driver to version 8.08.00.07.07.5-k1

Added support for the following:

- Handle cases for limiting Read Diagnostic Parameter (RDP) response payload length.
- Add fabric priority QoS (Quality of Service) lun (Logical Unit) IOCB (I/O Control Block) mechanism.
- Implement CT (Common Transport) command GFO (Get Fabric Object)
- Retry switch command on timed out.
- Add short name for SFP (Small Form-Factor Pluggable) range auto detect.
- Add ability to auto detect SFP (Small Form-Factor Pluggable) type.
- Add support for fabric priority per target.
- Allow Storage Name Service (SNS) fabric login to be retried.
- Increase the login retry count to 30.

Supported Devices and Features

This driver supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

Red Hat Enterprise Linux 7 Server FCoE Driver Kit for HPE Emulex(BRCM) Converged Network Adapters(CNAs) and mezzanine Converged Network Adapters(CNAs)
Version: 12.0.1110.11 **(Recommended)**
Filename: kmod-brcmfcoe-12.0.1110.11-1.rhel7u4.x86_64.compsig; kmod-brcmfcoe-12.0.1110.11-1.rhel7u4.x86_64.rpm; kmod-brcmfcoe-12.0.1110.11-1.rhel7u5.x86_64.compsig; kmod-brcmfcoe-12.0.1110.11-1.rhel7u5.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this

change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Added support for Red Hat Enterprise Linux 7u5

Updated to Driver version 12.0.1110.11

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HPE StoreFabric CN1200E-T Adapter

Red Hat Enterprise Linux 7 Server Fibre Channel Driver Kit for HPE Emulex Host Bus Adapters and mezzanine Host Bus Adapters
Version: 11.4.334.12 **(Recommended)**
Filename: kmod-elx-lpfc-11.4.334.12-1.rhel7u4.x86_64.compsig; kmod-elx-lpfc-11.4.334.12-1.rhel7u4.x86_64.rpm; kmod-elx-lpfc-11.4.334.12-1.rhel7u5.x86_64.compsig; kmod-elx-lpfc-11.4.334.12-1.rhel7u5.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Added support for Red Hat Enterprise Linux 7u5

Updated to driver version 11.4.334.12

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

SUSE Linux Enterprise Server 11 (AMD64/EM64T) FC Driver Kit for HPE Qlogic and mezzanine Host Bus Adapters
Version: 8.08.00.07.11.3-k1 **(Recommended)**
Filename: qlgc-qla2xxx-kmp-default-8.08.00.07.11.3_k1_3.0.101_63-1.sles11sp4.x86_64.compsig; qlgc-qla2xxx-kmp-default-8.08.00.07.11.3_k1_3.0.101_63-1.sles11sp4.x86_64.rpm; qlgc-qla2xxx-kmp-default-8.08.00.07.11.3_k1_3.0.76_0.11-1.sles11sp3.x86_64.compsig; qlgc-qla2xxx-kmp-default-8.08.00.07.11.3_k1_3.0.76_0.11-1.sles11sp3.x86_64.rpm; qlgc-qla2xxx-kmp-xen-8.08.00.07.11.3_k1_3.0.101_63-1.sles11sp4.x86_64.compsig; qlgc-qla2xxx-kmp-xen-8.08.00.07.11.3_k1_3.0.101_63-1.sles11sp4.x86_64.rpm; qlgc-qla2xxx-kmp-xen-8.08.00.07.11.3_k1_3.0.76_0.11-1.sles11sp3.x86_64.compsig; qlgc-qla2xxx-kmp-xen-8.08.00.07.11.3_k1_3.0.76_0.11-1.sles11sp3.x86_64.rpm

Important Note!

Release Notes

HPE StoreFabric QLogic Adapters Release Notes

Note: The rpm base-name for the QLogic driver has been changed to "qlgc". Upgrades from the earlier "hpqlgc" driver are supported.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Fixes

This driver version resolves the following:

- Mask off Scope bits in retry delay.
- Track if INQ (Inquiry) was sent, and send INQ (Inquiry) to all LUNs (Logical Unit).
- Prevent re_login trigger from sending too many commands
- Prevent multiple active discovery commands per session
- Correction to non-existent fabric name.
- Remove RDP (Read Diagnostic Parameter) response size cropping for logged out port.
- Fix supported speed ranges in FDMI/RDP (Fabric Device Management Interface /Read Diagnostic Parameter).
- GPID (Get Node Identification) Data unexpected terminations.
- Re-login for N-port Handle in use.
- Re-login is being triggered too fast.
- Reported supported link speeds.
- Add correction to fc (Fibre Channel) host stats (Statistics).

Enhancements

Updated driver version 8.08.00.07.11.3-k1

Added support for the following:

- Handle cases for limiting Read Diagnostic Parameter (RDP) response payload length.
- Add fabric priority QoS (Quality of Service) lun (Logical Unit) IOCB (I/O Control Block) mechanism.
- Implement CT (Common Transport) command GFO (Get Fabric Object)
- Retry switch command on timed out.
- Add short name for SFP (Small Form-Factor Pluggable) range auto detect.
- Add ability to auto detect SFP (Small Form-Factor Pluggable) type.
- Add support for fabric priority per target.
- Allow Storage Name Service (SNS) fabric login to be retried.
- Increase the login retry count to 30.

Supported Devices and Features

This driver supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

SUSE Linux Enterprise Server 11 (AMD64/EM64T) FCoE Driver Kit for HPE Emulex(BRCM) Converged Network Adapters(CNAs) and mezzanine Converged Network Adapters(CNAs)
Version: 12.0.1110.11 **(Recommended)**
Filename: brcmfcoe-kmp-default-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.compsig; brcmfcoe-kmp-default-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.rpm; brcmfcoe-kmp-default-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.compsig; brcmfcoe-kmp-default-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.rpm; brcmfcoe-kmp-trace-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.compsig; brcmfcoe-kmp-trace-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.rpm; brcmfcoe-kmp-trace-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.compsig; brcmfcoe-kmp-trace-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.rpm; brcmfcoe-kmp-xen-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.compsig; brcmfcoe-kmp-xen-12.0.1110.11_3.0.101_63-1.sles11sp4.x86_64.rpm; brcmfcoe-kmp-xen-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.compsig; brcmfcoe-kmp-xen-12.0.1110.11_3.0.76_0.11-1.sles11sp3.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent

software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to Driver version 12.0.1110.11

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HPE StoreFabric CN1200E-T Adapter

SUSE Linux Enterprise Server 11 (AMD64/EM64T) Fibre Channel Driver Kit for HPE Emulex Host Bus Adapters and mezzanine Host Bus Adapters Version: 11.4.334.12 **(Recommended)**
Filename: elx-lpfc-kmp-default-11.4.334.12_3.0.101_63-1.sles11sp4.x86_64.compsig; elx-lpfc-kmp-default-11.4.334.12_3.0.101_63-1.sles11sp4.x86_64.rpm; elx-lpfc-kmp-default-11.4.334.12_3.0.76_0.11-1.sles11sp3.x86_64.compsig; elx-lpfc-kmp-default-11.4.334.12_3.0.76_0.11-1.sles11sp3.x86_64.rpm; elx-lpfc-kmp-trace-11.4.334.12_3.0.101_63-1.sles11sp4.x86_64.compsig; elx-lpfc-kmp-trace-11.4.334.12_3.0.101_63-1.sles11sp4.x86_64.rpm; elx-lpfc-kmp-trace-11.4.334.12_3.0.76_0.11-1.sles11sp3.x86_64.compsig; elx-lpfc-kmp-trace-11.4.334.12_3.0.76_0.11-1.sles11sp3.x86_64.rpm; elx-lpfc-kmp-xen-11.4.334.12_3.0.101_63-1.sles11sp4.x86_64.compsig; elx-lpfc-kmp-xen-11.4.334.12_3.0.101_63-1.sles11sp4.x86_64.rpm; elx-lpfc-kmp-xen-11.4.334.12_3.0.76_0.11-1.sles11sp3.x86_64.compsig; elx-lpfc-kmp-xen-11.4.334.12_3.0.76_0.11-1.sles11sp3.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals

2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated driver version to 11.4.334.12

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

SUSE Linux Enterprise Server 12 FC Driver Kit for HPE QLogic and mezzanine Host Bus Adapters
Version: 8.08.00.07.12.3-k1 **(Recommended)**
Filename: qlgc-qla2xxx-kmp-default-8.08.00.07.12.2_k1_k4.4.21_69-1.sles12sp2.x86_64.compsig; qlgc-qla2xxx-kmp-default-8.08.00.07.12.2_k1_k4.4.21_69-1.sles12sp2.x86_64.rpm; qlgc-qla2xxx-kmp-default-8.08.00.07.12.3_k1_k4.4.73_5-1.sles12sp3.x86_64.compsig; qlgc-qla2xxx-kmp-default-8.08.00.07.12.3_k1_k4.4.73_5-1.sles12sp3.x86_64.rpm

Important Note!

Release Notes:

HPE StoreFabric QLogic Adapters Release Notes

Note: The rpm base-name for the QLogic driver has been changed to "qlgc". Upgrades from the earlier "hpqlgc" driver are supported.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Fixes

This driver version resolves the following:

- Mask off Scope bits in retry delay.
- Track if INQ (Inquiry) was sent, and send INQ (Inquiry) to all LUNs (Logical Unit).
- Prevent re_login trigger from sending too many commands
- Prevent multiple active discovery commands per session
- Correction to non-existent fabric name.
- Remove RDP (Read Diagnostic Parameter) response size cropping for logged out port.
- Fix supported speed ranges in FDMI/RDP (Fabric Device Management Interface /Read Diagnostic Parameter).
- GPID (Get Node Identification) Data unexpected terminations.
- Re-login for N-port Handle in use.
- Re-login is being triggered too fast.
- Reported supported link speeds.
- Add correction to fc (Fibre Channel) host stats (Statistics).

Enhancements

Updated to version 8.08.00.07.12.3-k1

Added support for the following:

- Handle cases for limiting Read Diagnostic Parameter (RDP) response payload length.
- Add fabric priority QoS (Quality of Service) lun (Logical Unit) IOCB (I/O Control Block) mechanism.
- Implement CT (Common Transport) command GFO (Get Fabric Object)
- Retry switch command on timed out.
- Add short name for SFP (Small Form-Factor Pluggable) range auto detect.
- Add ability to auto detect SFP (Small Form-Factor Pluggable) type.
- Add support for fabric priority per target.
- Allow Storage Name Service (SNS) fabric login to be retried.
- Increase the login retry count to 30.

Supported Devices and Features

This driver supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

SUSE Linux Enterprise Server 12 FCoE Driver Kit for HPE Emulex(BRCM) Converged Network Adapters(CNAs) and mezzanine Converged Network Adapters(CNAs)
Version: 12.0.1110.11 **(Recommended)**
Filename: brcmfcoe-kmp-default-12.0.1110.11_k4.4.21_69-1.sles12sp2.x86_64.compsig; brcmfcoe-kmp-default-12.0.1110.11_k4.4.21_69-1.sles12sp2.x86_64.rpm; brcmfcoe-kmp-default-12.0.1110.11_k4.4.73_5-1.sles12sp3.x86_64.compsig; brcmfcoe-kmp-default-12.0.1110.11_k4.4.73_5-1.sles12sp3.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this

change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to Driver version 12.0.1110.11

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HPE StoreFabric CN1200E-T Adapter

SUSE Linux Enterprise Server 12 Fibre Channel Driver Kit for HPE Emulex Host Bus Adapters and mezzanine Host Bus Adapters
Version: 11.4.334.12 **(Recommended)**
Filename: elx-lpfc-kmp-default-11.4.334.12_k4.4.103_6.38-1.sles12sp3.x86_64.compsig; elx-lpfc-kmp-default-11.4.334.12_k4.4.103_6.38-1.sles12sp3.x86_64.rpm; elx-lpfc-kmp-default-11.4.334.12_k4.4.21_69-1.sles12sp2.x86_64.compsig; elx-lpfc-kmp-default-11.4.334.12_k4.4.21_69-1.sles12sp2.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please Update SuSE Linux Enterprise Server 12 service pack 3(SLES 12sp3) Operating System with latest Errata Kernel.

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to driver version 11.4.334.12

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

Driver - System Top

HPE NVDIMM-N Drivers for Microsoft Windows Server 2012 and 2012 R2
Version: 2.0.0.2 **(Recommended)**
Filename: cp031329.compsig; cp031329.exe

Enhancements

These NVDIMM-N drivers enable support for Persistent Memory technology on select HPE Servers running Microsoft Windows Server 2012 and 2012 R2.

- Added support for HPE 16GB NVDIMM devices.
- Changed block sector size from 512B to 4096B. Old data won't be accessible and must be backed up first if it needs to be preserved.

For more information about Persistent Memory technology offered on HPE Servers, please consult the following links:

- https://www.hpe.com/us/en/servers/persistent-memory.html
- http://h20195.www2.hpe.com/V2/GetDocument.aspx?docname=4AA6-4681ENW&cc=us&lc=en

---

Driver - System Management Top

HPE ProLiant Gen9 Chipset Identifier for Windows Server 2012 to Server 2016
Version: 10.1.2.77 (B) **(Optional)**
Filename: cp035099.exe

Fixes

Corrected a potential installation failure that could occur when Windows Device Guard is enabled.

---

iLO 3/4 Channel Interface Driver for Windows Server 2008 to Server 2012 R2
Version: 3.30.0.0 **(Optional)**
Filename: cp029394.exe

Important Note!

The Channel Interface Driver was separated into its own component when the ProLiant Support Pack version 9.00 was released. Previously, the driver was a part of the *iLO 3 Management Controller Driver Package* component.

Fixes

Ensure that work items created by the driver are properly terminated if the driver has been restarted.

iLO 3/4 Management Controller Driver Package for Windows Server 2008 to Server 2012 R2
Version: 3.30.0.0 **(Optional)**
Filename: cp029429.exe

Prerequisites

The *iLO 3/4 Channel Interface Driver for Windows Server 2008 to Server 2012 R2* (version 3.4.0.0 or later) must be installed prior to this component. The Channel Interface Driver was previously included within this component, but is now installed separately.

Enhancements

The support provided by the ProLiant System Shutdown service has been merged into the ProLiant Monitor service. The ProLiant System Shutdown service will no longer appear as a separate item in the list of services on the system.

---

iLO 3/4 Management Controller Driver Package for Windows Server 2016
Version: 3.30.0.0 **(Optional)**
Filename: cp030672.exe

Prerequisites

The *iLO 3/4 Channel Interface Driver for Windows Server 2016* must be installed prior to this component.

Enhancements

Initial release to support Windows Server 2016.

---

iLO 4 Channel Interface Driver for Windows Server 2016
Version: 3.31.0.0 **(Recommended)**
Filename: cp034683.exe

Fixes

Corrected a Windows bugcheck (DPC_WATCHDOG_VIOLATION) that could occur if iLO Remote Console or iLO Virtual Media are in use.

---

iLO 5 Automatic Server Recovery Driver for Windows Server 2012 R2
Version: 4.2.0.0 (B) **(Optional)**
Filename: cp034068.compsig; cp034068.exe

Important Note!

Installing the iLO 5 Channel Interface Driver, version 4.1.0.0 or earlier, will overwrite this driver. To avoid the overwrite, use version 4.1.0.0(B) or later of the iLO 5 Channel Interface Driver.

Enhancements

Added support for the HPE ProLiant DL325 Gen10.

---

iLO 5 Automatic Server Recovery Driver for Windows Server 2016
Version: 4.2.0.0 (B) **(Optional)**
Filename: cp034069.compsig; cp034069.exe

Important Note!

Installing the iLO 5 Channel Interface Driver, version 4.1.0.0 or earlier, will overwrite this driver. To avoid the overwrite, use version 4.1.0.0(B) or later of the iLO 5 Channel Interface Driver.

Enhancements

Added support for the HPE ProLiant DL325 Gen10.

---

iLO 5 Channel Interface Driver for Windows Server 2012 R2
Version: 4.3.0.0 **(Optional)**
Filename: cp034070.compsig; cp034070.exe

Enhancements

- Enabled message-signaled interrupts to avoid interrupt sharing with the Universal Serial Bus controller in iLO 5.
-

Added support for the HPE ProLiant DL325 Gen10.

iLO 5 Channel Interface Driver for Windows Server 2016
Version: 4.3.0.0 **(Optional)**
Filename: cp034071.compsig; cp034071.exe

Enhancements

- Enabled message-signaled interrupts to avoid interrupt sharing with the Universal Serial Bus controller in iLO 5.
- Added support for the HPE ProLiant DL325 Gen10.

Driver - Video

Top

Matrox G200eH Video Controller Driver for Windows Server 2012 and Server 2012 R2
Version: 9.15.1.184 **(Optional)**
Filename: cp032302.exe

Enhancements

Improved video performance compared to the 9.15.1.174 release.

Matrox G200eH Video Controller Driver for Windows Server 2016
Version: 9.15.1.184 **(Optional)**
Filename: cp032303.exe

Enhancements

Improved video performance compared to the 9.15.1.174 release.

Matrox G200eH3 Video Controller Driver for Windows Server 2012 R2
Version: 9.15.1.184 (B) **(Optional)**
Filename: cp033123.compsig; cp033123.exe

Enhancements

Added support for the HPE ProLiant DL325 Gen10.

Matrox G200eH3 Video Controller Driver for Windows Server 2016
Version: 9.15.1.184 (B) **(Optional)**
Filename: cp033124.compsig; cp033124.exe

Enhancements

Added support for the HPE ProLiant DL325 Gen10.

Firmware - Blade Infrastructure

Top

HPE BladeSystem c-Class Virtual Connect Firmware, Ethernet plus 8Gb 20-port and 8/16Gb 24-port FC Edition Component for Windows
Version: 4.62 **(Recommended)**
Filename: cp034382.exe

Prerequisites

The 4.62 version of HPE Virtual Connect Release Notes contains the prerequisites and can also be found in the following URL: http://www.hpe.com/info/vc/manuals

Fixes

The list of issues resolved in 4.62 version can be found in the HPE Virtual Connect Release Notes at URL: http://www.hpe.com/info/vc/manuals

Enhancements

The list of enhancements in 4.62 version can be found in the HPE Virtual Connect Release Notes at URL: http://www.hpe.com/info/vc/manuals

Supported Devices and Features

HPE Flex-10 10Gb Virtual Connect Ethernet Module for c-Class BladeSystem

HPE Virtual Connect FlexFabric 10Gb/24-port Module for c-Class BladeSystem

HPE Virtual Connect 8Gb 24-port Fibre Channel Module for c-Class BladeSystem

HPE Virtual Connect 8Gb 20-port Fibre Channel Module for c-Class BladeSystem

HPE Virtual Connect Flex-10/10D Module for c-Class BladeSystem

HPE Virtual Connect FlexFabric-20/40 F8 Module for HP BladeSystem c-Class HPE

Virtual Connect 16Gb 24-port Fibre Channel Module for c-Class BladeSystem

---

HPE BladeSystem c-Class Virtual Connect Firmware, Ethernet plus 8Gb 20-port and 8/16Gb 24-port FC Edition Component for Linux
Version: 4.62 **(Recommended)**
Filename: RPMS/i386/firmware-vceth-4.62-1.1.i386.rpm

Prerequisites

The 4.62 version of HPE Virtual Connect Release Notes contains the prerequisites and can be found in the following URL: http://www.hpe.com/info/vc/manuals

Fixes

The list of issues resolved in 4.62 version can be found in the HPE Virtual Connect Release Notes at URL: http://www.hpe.com/info/vc/manuals

Enhancements

The list of enhancements in 4.62 version can be found in the HPE Virtual Connect Release Notes at URL: http://www.hpe.com/info/vc/manuals

Supported Devices and Features

HPE Flex-10 10Gb Virtual Connect Ethernet Module for c-Class BladeSystem

HPE Virtual Connect FlexFabric 10Gb/24-port Module for c-Class BladeSystem

HPE Virtual Connect 8Gb 24-port Fibre Channel Module for c-Class BladeSystem

HPE Virtual Connect 8Gb 20-port Fibre Channel Module for c-Class BladeSystem

HPE Virtual Connect Flex-10/10D Module for c-Class BladeSystem

HPE Virtual Connect FlexFabric-20/40 F8 Module for HP BladeSystem c-Class HPE

Virtual Connect 16Gb 24-port Fibre Channel Module for c-Class BladeSystem

---

Online HP 6Gb SAS BL Switch Firmware Smart Component for Linux (x86/x64)
Version: 4.3.6.0 **(Optional)**
Filename: RPMS/i586/firmware-solex6gb-solex-4.3.6.0-1.1.i586.rpm

Enhancements

- Initial drop for Snap3

Online HPE 6Gb SAS BL Switch Firmware Smart Component for Windows (x86/x64)
Version: 4.3.6.0 **(Optional)**
Filename: cp034920.exe

Enhancements

- Initial drop for Snap3

Online HPE BladeSystem c-Class Onboard Administrator Firmware Component for Linux
Version: 4.70 **(Optional)**
Filename: RPMS/x86_64/firmware-oa-4.70-1.1.x86_64.rpm

Important Note!

Update to this firmware version if any documented fixes or enhanced functionality provided by this version would be useful to your system.

Important Notes

- **Firmware Upgrade**

Starting OA 4.50 release, a standardized code signing and validation mechanism has been introduced to enhance the firmware image authenticity.
    - For customers using Firmware ROM image to upgrade OA:
        - For OAs with firmware version less than 3.50, first update to OA 3.50 and then continue updating to OA 4.50 or above.
    - For customers using Smart Components to upgrade OA:
        - OA firmware update mechanisms which rely on HPE Smart Components (example: EFM), will not be affected by this change. The Smart Component will automatically perform the intermediate upgrade to OA 3.50 before performing the OA 4.50 or above upgrade.

- **EFM**
    - The OA only supports SPP ISO images that are less than 4 GB in size, whether hosted directly via the Enclosure DVD feature or an attached USB key, or mounted remotely via a specified URL. If an ISO image exceeds 4 GB, the CLI SHOW FIRMWARE MANAGEMENT command displays ISO URL Status as "Invalid URL."
    - If an SPP ISO image exceeds 4 GB, it is necessary to create a custom ISO image that excludes components unnecessary to the OA EFM blade firmware update process. At a minimum, the custom ISO must contain the firmware components for HPE ProLiant BL servers. (When using HP SUM to create the custom ISO image, select Firmware as the Component Type, and select HPE ProLiant BL Series as the Server Type.) For information about creating a custom ISO image compatible for OA EFM functionality, see the *HPE BladeSystem Onboard Administrator User Guide*. More HP SUM information can be found via HPE Smart Update Manager online help or at www.hpe.com/info/hpsum/documentation.

- **FIPS**
    - OA 3.71 is in active evaluation for FIPS as referenced in the 140-2 In Process list located at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf.

- **IPv6**
    - When the Enable DHCPv6 or Enable SLAAC enclosure IPv6 settings are disabled on the Onboard Administrator, the respective DHCPv6 or SLAAC addresses of the iLOs in the enclosure are retained until these addresses expire automatically based on their respective configurations. A manual reset of the iLO releases these addresses immediately

Prerequisites

The Onboard Administrator Smart Component contains 32-bit executable binaries. As a result, the client operating system upon which the OA Smart Component is installed and executed must either have native support for 32-bit executables or must have the 32-bit compatibility libraries installed.

Fixes

General

- Addressed an issue where OA "update iLO all" command fails in an enclosure with maximum Blades.
- Addressed an issue where a Warning Alert was wrongly sent when a fan is reseated in an enclosure
- Addressed an issue where the port mapping information for 560M Izzy adapter Mezz controller was not displayed correctly.
- Addressed an issue where Remote Syslog logging would fail when OA failover happened in an IPv6 only environment.
- Enhanced OA to bring the server from a power throttled state back to normal power state upon an OA reboot to circumvent an unwarranted emergency brake.
- Fixed an issue where the Active and Standby OAs can have the same IP address in some rare situations.
- Resolved an issue where a Gen9 server's host name gets cleared when the blade is rebooted.
- Addressed an issue where server blade Power ON will be delayed in enclosures with OA Firmware Version 4.60 and managed by HPE OneView, when the OA module is reset until OneView refreshes the servers.

Security

The following security vulnerabilities were fixed:

- CVE-2016-5387– Addressed a vulnerability which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request.
- CVE-2016-2183- Addressed a vulnerability against TLS ciphers with 64bit block size in which makes it easier for remote attackers to obtain cleartext data via an attack against a long-duration encrypted session
- CVE-2016-6515 - Addressed a vulnerability in OpenSSH which did not limit password lengths for password authentication, which allows remote attackers to cause a denial of service via a long string.
- CVE-2015-8215 - Addressed a vulnerability IPv6 stack which does not validate attempted changes to the MTU value, which allows context-dependent attackers to cause a denial of service.
- Addressed issue where in Onboard Administrator was vulnerable to Buffer overflow.
- Added the HSTS[HTTP strict transport security] support in OA.
- Addressed a memory corruption vulnerability in the post-authentication sshd process.

Issues and workarounds

Browsers

- OA GUI is not accessible in Chrome versions 43.0.2357.10 to 44.0.2383.The issue was caused by a "regression" in Chrome (or WebKit). Customers should use an alternative browser like Firefox or Internet Explorer or try a different version of Chrome.
- SSO-to-iLO connection from the OA using an iLO host name fails with Microsoft Internet Explorer11 on Windows 8.On a Windows 8 system with Internet Explorer 10 or Internet Explorer 11, if the OA web GUI session is loaded using a host name instead of an IP address, an attempt to open an iLO window using SSO from the OA web GUI might result in the iLO page loading in the OA web GUI window instead of the intended new window. This issue was determined to be a bug in Internet Explorer and is expected to be fixed in a future release or update for Internet Explorer. To work around this issue, either use an IP address to load the OA Web GUI, or turn off Protected Mode for the appropriate zone in Internet Explorer's settings. This issue occurs only on Internet Explorer browsers.

FIPS

Certificates smaller than 2048 bits in size are not compliant with FIPS requirements as enforced by the OA firmware starting with OA 4.20. When the OA running OA firmware version 4.40 or greater is operating in FIPS Mode ON/DEBUG and is configured with a 1024-

bit LDAP certificate that was installed when running a previous version of OA firmware, FIPS Mode ON/DEBUG is considered to be operating in a degraded state due to the presence of the non-compliant certificate. While operating in this FIPS-Degraded Mode operational state, attempts to set FIPS Mode OFF from the OA GUI Network Access>FIPS tab will fail and show the error message The selected FIPS mode is already enabled. When the non-compliant certificate is removed, the FIPS-Degraded operational status is cleared, FIPS Mode can then be successfully set to OFF from the GUI interface. Note that the OA CLI command SET FIPS MODE OFF can be successfully used to set FIPS Mode OFF even with non-compliant 1024-bit LDAP certificates installed in the OA.

IRC

Unable to open .net IRC console for Gen10 Blades, Gen9 Blades also have the same issue. The Java applet and Webstart however, loads but the virtual media mounting fails. The work around is to launch the IRC through IRC Application (HP Lights-Out Stand Alone Remote Console) which is installed on terminal client.

EFM

To use EFM on Gen 10 Blades, please select options/filters "*Make Bootable ISO file" and "Enclosure Firmware Management"* while creating custom SPP ISO on HPSUM 8.0.0. Please refer to HPSUM 8.0.0 User guide for further details.

Enhancements

Onboard Administrator 4.70 provides support for the following enhancements:

Hardware additions

- BL460c Gen 10.
- HPE 10GbE Pass-Thru Module.
- Qualified support for HPE Integrity BL8x0c i6 Server Blade.

Features**: additions and changes**

General

- Added support for Gen 10 Server and iLO5 features.
- Added support for the enhanced KVM functionality in iLO5
- Added support for HTTP boot option in the server boot options
- Add support for HPE 10GbE Pass-Thru interconnect module.
- Added support for HPE Integrity BL8x0c i6 Server Blade.
- GUI, CLI, Smart components, help files, URLs, and product names rebranded to align with HPE branding guidelines.
- Added a new SNMP trap to indicate that the power redundancy is restored in the enclosure.
- Enhanced "SHOW ENCLOSURE TEMP" command output, to display the temperature readings like Current, Caution and Critical temperature threshold values for interconnect modules.
- Added a provision to make sysName field to be set to DNS host name for the traps sent from Onboard Administrator.

Security

- Adding support for CNSA approved algorithms and a new security mode - TOP_SECRET.
- Added the ability to Enable/Disable cipher/protocol in FIPS OFF mode.
- Added support for secured communication between HPE Embedded Remote Support functionality and the HPE Support Datacenters with the use of SHA-2 certificates.

Online HPE BladeSystem c-Class Onboard Administrator Firmware Component for Linux
Version: 4.85 **(Recommended)**
Filename: RPMS/x86_64/firmware-oa-4.85-1.1.x86_64.rpm

Important Note!

Important Notes

- **Firmware Upgrade**
  - Starting OA 4.50 release, a standardized code signing and validation mechanism has been introduced to enhance the firmware image authenticity.
  - For customers using Firmware ROM image to upgrade OA:
    - For OAs with firmware version less than 3.50, first update to OA 3.50 and then continue updating to OA 4.50 or above.
  - For customers using Smart Components to upgrade OA:
    - OA firmware update mechanisms which rely on HPE Smart Components (example: EFM), will not be affected by this change. The Smart Component will automatically perform the intermediate upgrade to OA 3.50 before performing the OA 4.50 or above upgrade.
- **EFM**
  - The OA only supports SPP ISO images that are less than 4 GB in size, whether hosted directly via the Enclosure DVD feature or an attached USB key, or mounted remotely via a specified URL. If an ISO image exceeds 4 GB, the CLI SHOW FIRMWARE MANAGEMENT command displays ISO URL Status as "Invalid URL."
  - If an SPP ISO image exceeds 4 GB, it is necessary to create a custom ISO image that excludes components unnecessary to the OA EFM blade firmware update process. At a minimum, the custom ISO must contain the firmware components for HPE ProLiant BL servers. (When using HP SUM to create the custom ISO image, select Firmware as the Component Type, and select HPE ProLiant BL Series as the Server Type.) For information about creating a custom ISO image compatible for OA EFM functionality, see the *HPE BladeSystem Onboard Administrator User Guide*. More HP SUM information can be found via HPE Smart Update Manager online help or at https://www.hpe.com/servers/hpsum/documentation.
- **FIPS**
  - OA 4.40 is in active evaluation for FIPS as referenced in the 140-2 In Process list located at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf.

- **IPv6**
  - When the Enable DHCPv6 or Enable SLAAC enclosure IPv6 settings are disabled on the Onboard Administrator, the respective DHCPv6 or SLAAC addresses of the iLOs in the enclosure are retained until these addresses expire automatically based on their respective configurations. A manual reset of the iLO releases these addresses immediately

Prerequisites

The Onboard Administrator Smart Component contains 32-bit executable binaries. As a result, the client operating system upon which the OA Smart Component is installed and executed must either have native support for 32-bit executables or must have the 32-bit compatibility libraries installed.

Fixes

General

- Addressed an issue where SNMP trap cpqRackEnclosureManagerLinkUp was not sent after an Onboard Administrator failover.
- Addressed online help content issues seen in the previous version of Onboard Administrator.

Security

The following security vulnerabilities were fixed:

- CVE-2017-8105 - Addressed a memory corruption vulnerability caused by a buffer overflow.
- CVE-2016-10244 – Addressed a vulnerability which might allow a remote attacker to cause denial-of-service via a crafted file.

Issues and workarounds

Browsers

- OA GUI is not accessible in Chrome versions 43.0.2357.10 to 44.0.2383.The issue was caused by a "regression" in Chrome (or WebKit). Customers should use an alternative browser like Firefox or Internet Explorer or try a different version of Chrome.
- SSO-to-iLO connection from the OA using an iLO host name fails with Microsoft Internet Explorer11 on Windows 8. On a Windows 8 system with Internet Explorer 10 or Internet Explorer 11, if the OA web GUI session is loaded using a host name instead of an IP address, an attempt to open an iLO window using SSO from the OA web GUI might result in the iLO page loading in the OA web GUI window instead of the intended new window. This issue was determined to be a bug in Internet Explorer and is expected to be fixed in a future release or update for Internet Explorer. To work around this issue, either use an IP address to load the OA Web GUI, or turn off Protected Mode for the appropriate zone in Internet Explorer's settings. This issue occurs only on Internet Explorer browsers.

FIPS

Certificates smaller than 2048 bits in size are not compliant with FIPS requirements as enforced by the OA firmware starting with OA 4.20. When the OA running OA firmware version 4.40 or greater is operating in FIPS Mode ON/DEBUG and is configured with a 1024-bit LDAP certificate that was installed when running a previous version of OA firmware, FIPS Mode ON/DEBUG is considered to be operating in a degraded state due to the presence of the non-compliant certificate. While operating in this FIPS-Degraded Mode operational state, attempts to set FIPS Mode OFF from the OA GUI Network Access>FIPS tab will fail and show the error message The selected FIPS mode is already enabled. When the non-compliant certificate is removed, the FIPS-Degraded operational status is cleared, FIPS Mode can then be successfully set to OFF from the GUI interface. Note that the OA CLI command SET FIPS MODE OFF can be successfully used to set FIPS Mode OFF even with non-compliant 1024-bit LDAP certificates installed in the OA.

IRC

Unable to open .net IRC console for Gen10 Blades, Gen9 Blades also have the same issue. The Java applet and Webstart however, loads but the virtual media mounting fails. The work around is to launch the IRC through IRC Application (HP Lights-Out Stand Alone Remote Console) which is installed on terminal client.

EFM

To use EFM on Gen 10 Blades, please select options/filters "*Make Bootable ISO file" and "Enclosure Firmware Management"* while creating custom SPP ISO on HPSUM 8.0.0. Please refer to HPSUM 8.0.0 User guide for further details.

CAC

- In the CAC mode SSH, Telnet and XML Reply protocols will be disabled.
- Linked enclosure login will not work if the linked enclosure in CAC mode.
- If accurate Service account details are not provided, LDAP user login with certificate will fail.
- It is highly recommended to establish a recovery plan before getting started with CAC. If something goes wrong with the OA configuration, the OA may be recovered through the serial port or Insight Display panel and USB KEY. Both methods require physical access to the OA. However, if an LCD PIN has been configured (and forgotten) and local accounts have been disabled or CAC has been incorrectly configured then, the only way to recover is through a serial port. The two most common situations where OA recovery is needed are when LDAP has been configured incorrectly with local accounts disabled or when CAC has been configured without certificate access.

Configurable SSH Port Number

If a Standby OA is running firmware version less than 4.85 and it is updated to firmware version greater than or equal to 4.85 using synchronize firmware feature from Active OA, after the firmware update and reboot of the Standby OA, SSH port will not open in the configured port number. The work around is to reboot the Standby OA and SSH port will open in the configured port in next boot. This issue will not occur in the case where SSH port is configured to default port 22 in the Active OA.

Enhancements

Onboard Administrator 4.85 provides support for the following enhancements:

Hardware additions

- HPE D2500sb Storage Blade

Features**: additions and changes**

General

- Onboard Administrator has been enhanced to allow configuring an IPv6 address as SNMP EngineID.
- Onboard Administrator has been enhanced to allow configuring a user defined SSH port number. This will allow users to configure a non-standard SSH port instead of the default SSH port 22.

Security

General Data Protection Requirements (GDPR) support added in Onboard Administrator for HPE Embedded Remote Support solution. The HPE passport username will now be stored in an encrypted form.

Online HPE BladeSystem c-Class Onboard Administrator Firmware Component for Windows
Version: 4.85 **(Recommended)**
Filename: cp034861.exe

Important Note!

Important Notes

- **Firmware Upgrade**
  - Starting OA 4.50 release, a standardized code signing and validation mechanism has been introduced to enhance the firmware image authenticity.
  - For customers using Firmware ROM image to upgrade OA:
    - For OAs with firmware version less than 3.50, first update to OA 3.50 and then continue updating to OA 4.50 or above.
  - For customers using Smart Components to upgrade OA:
    - OA firmware update mechanisms which rely on HPE Smart Components (example: EFM), will not be affected by this change. The Smart Component will automatically perform the intermediate upgrade to OA 3.50 before performing the OA 4.50 or above upgrade.
- **EFM**
  - The OA only supports SPP ISO images that are less than 4 GB in size, whether hosted directly via the Enclosure DVD feature or an attached USB key, or mounted remotely via a specified URL. If an ISO image exceeds 4 GB, the CLI SHOW FIRMWARE MANAGEMENT command displays ISO URL Status as "Invalid URL."
  - If an SPP ISO image exceeds 4 GB, it is necessary to create a custom ISO image that excludes components unnecessary to the OA EFM blade firmware update process. At a minimum, the custom ISO must contain the firmware components for HPE ProLiant BL servers. (When using HP SUM to create the custom ISO image, select Firmware as the Component Type, and select HPE ProLiant BL Series as the Server Type.) For information about creating a custom ISO image compatible for OA EFM functionality, see the *HPE BladeSystem Onboard Administrator User Guide*. More HP SUM information can be found via HPE Smart Update Manager online help or at https://www.hpe.com/servers/hpsum/documentation.
- **FIPS**
  - OA 4.40 is in active evaluation for FIPS as referenced in the 140-2 In Process list located at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf.
- **IPv6**
  - When the Enable DHCPv6 or Enable SLAAC enclosure IPv6 settings are disabled on the Onboard Administrator, the respective DHCPv6 or SLAAC addresses of the iLOs in the enclosure are retained until these addresses expire automatically based on their respective configurations. A manual reset of the iLO releases these addresses immediately.

Prerequisites

The Onboard Administrator Smart Component contains 32-bit executable binaries. As a result, the client operating system upon which the OA Smart Component is installed and executed must either have native support for 32-bit executables or must have the 32-bit compatibility libraries installed.

Fixes

General

- Addressed an issue where SNMP trap cpqRackEnclosureManagerLinkUp was not sent after an Onboard Administrator failover.
- Addressed online help content issues seen in the previous version of Onboard Administrator.

Security

The following security vulnerabilities were fixed:

- CVE-2017-8105 - Addressed a memory corruption vulnerability caused by a buffer overflow.
- CVE-2016-10244 – Addressed a vulnerability which might allow a remote attacker to cause denial-of-service via a crafted file.

Issues and workarounds

Browsers

- OA GUI is not accessible in Chrome versions 43.0.2357.10 to 44.0.2383.The issue was caused by a "regression" in Chrome (or WebKit). Customers should use an alternative browser like Firefox or Internet Explorer or try a different version of Chrome.

- SSO-to-iLO connection from the OA using an iLO host name fails with Microsoft Internet Explorer11 on Windows 8. On a Windows 8 system with Internet Explorer 10 or Internet Explorer 11, if the OA web GUI session is loaded using a host name instead of an IP address, an attempt to open an iLO window using SSO from the OA web GUI might result in the iLO page loading in the OA web GUI window instead of the intended new window. This issue was determined to be a bug in Internet Explorer and is expected to be fixed in a future release or update for Internet Explorer. To work around this issue, either use an IP address to load the OA Web GUI, or turn off Protected Mode for the appropriate zone in Internet Explorer's settings. This issue occurs only on Internet Explorer browsers.

FIPS

Certificates smaller than 2048 bits in size are not compliant with FIPS requirements as enforced by the OA firmware starting with OA 4.20. When the OA running OA firmware version 4.40 or greater is operating in FIPS Mode ON/DEBUG and is configured with a 1024-bit LDAP certificate that was installed when running a previous version of OA firmware, FIPS Mode ON/DEBUG is considered to be operating in a degraded state due to the presence of the non-compliant certificate. While operating in this FIPS-Degraded Mode operational state, attempts to set FIPS Mode OFF from the OA GUI Network Access>FIPS tab will fail and show the error message The selected FIPS mode is already enabled. When the non-compliant certificate is removed, the FIPS-Degraded operational status is cleared, FIPS Mode can then be successfully set to OFF from the GUI interface. Note that the OA CLI command SET FIPS MODE OFF can be successfully used to set FIPS Mode OFF even with non-compliant 1024-bit LDAP certificates installed in the OA.

IRC

Unable to open .net IRC console for Gen10 Blades, Gen9 Blades also have the same issue. The Java applet and Webstart however, loads but the virtual media mounting fails. The work around is to launch the IRC through IRC Application (HP Lights-Out Stand Alone Remote Console) which is installed on terminal client.

EFM

To use EFM on Gen 10 Blades, please select options/filters "*Make Bootable ISO file" and* "*Enclosure Firmware Management"* while creating custom SPP ISO on HPSUM 8.0.0. Please refer to HPSUM 8.0.0 User guide for further details.

CAC

- In the CAC mode SSH, Telnet and XML Reply protocols will be disabled.
- Linked enclosure login will not work if the linked enclosure in CAC mode.
- If accurate Service account details are not provided, LDAP user login with certificate will fail.
- It is highly recommended to establish a recovery plan before getting started with CAC. If something goes wrong with the OA configuration, the OA may be recovered through the serial port or Insight Display panel and USB KEY. Both methods require physical access to the OA. However, if an LCD PIN has been configured (and forgotten) and local accounts have been disabled or CAC has been incorrectly configured then, the only way to recover is through a serial port. The two most common situations where OA recovery is needed are when LDAP has been configured incorrectly with local accounts disabled or when CAC has been configured without certificate access.

Configurable SSH Port Number

If a Standby OA is running firmware version less than 4.85 and it is updated to firmware version greater than or equal to 4.85 using synchronize firmware feature from Active OA, after the firmware update and reboot of the Standby OA, SSH port will not open in the configured port number. The work around is to reboot the Standby OA and SSH port will open in the configured port in next boot. This issue will not occur in the case where SSH port is configured to default port 22 in the Active OA.

Enhancements

Onboard Administrator 4.85 provides support for the following enhancements:

Hardware additions

- HPE D2500sb Storage Blade

Features**: additions and changes**

General

- Onboard Administrator has been enhanced to allow configuring an IPv6 address as SNMP EngineID.
- Onboard Administrator has been enhanced to allow configuring a user defined SSH port number. This will allow users to configure a non-standard SSH port instead of the default SSH port 22.

Security

General Data Protection Requirements (GDPR) support added in Onboard Administrator for HPE Embedded Remote Support solution. The HPE passport username will now be stored in an encrypted form.

Firmware - Lights-Out Management Top

Online ROM Flash Component for Linux - HPE Integrated Lights-Out 4
Version: 2.60 **(Critical)**
Filename: CP033806.scexe; RPMS/i386/hp-firmware-ilo4-2.60-1.1.i386.rpm

Important Note!

Install this update to take advantage of significant improvements to the write algorithm for the embedded 4 GB non-volatile flash memory (also known as the NAND). These improvements increase the NAND lifespan.

IPv6 network communications - Dedicated network connection only

Supported Networking Features
- IPv6 Static Address Assignment
- IPv6 SLAAC Address Assignment
- IPv6 Static Route Assignment
- IPv6 Static Default Gateway Entry
- DHCPv6 Stateful Address Assignment
- DHCPv6 Stateless DNS, Domain Name, and NTP Configuration
- Integrated Remote Console
- OA Single Sign-On
- HP-SIM Single Sign-On
- Web Server
- SSH Server
- SNTP Client
- DDNS Client
- RIBCL over IPv6
- SNMP
- AlertMail
- Remote Syslog
- WinDBG Support
- CPQLOCFG/HPLOMIG over an IPv6 connection
- Scriptable Virtual Media
- CLI/RIBCL Key Import over IPv6
- Authentication using LDAP and Kerberos over IPv6
- iLO Federation

Networking Features not supported by IPv6 in this release
- IPv6 Over Shared Network Port Connections
- IPMI
- NETBIOS-WINS
- Enterprise Secure Key Manager (ESKM) Support
- Embedded Remote Support (ERS)

Prerequisites

Hewlett Packard Enterprise recommends upgrading to the minimum versions of the iLO utilities:

- RESTful Interface Tool (iLOREST) 2.3
- HPQLOCFG v5.2
- Lights-Out XML Scripting Sample bundle 5.10.0
- HPONCFG Windows 5.2.0
- HPONCFG Linux 5.3.0
- LOCFG v5.10.0
- HPLOMIG 5.2.0

Fixes

The following issues are resolved in this version:

- iLO 4 unexpectedly restored itself to factory default settings when an user did not initiate the process.
- When Auto Power-On is set to Always Power On to Restore Last Power State, the server might not power on after a cold reset.
- False nonvolatile flash memory (NAND) test failures might occur after a firmware upgrade.
- Incorrect RAM and Storage values are displayed on the HPE OneView for VMware vCenter tab.
- Remote Support disk events include the text "Not Available" for the variables when data is missing.
- Some Power Supply information is missing from the iLO web interface.
- iLO displays Failed status instead of Disabled status when the Smart Array Cache Module battery is disconnected.
- An iLO SSH port disconnection issue was observed after more than two days of continuous operation.
- Values do not move up when the preceding entries in the Directory User Context fields are cleared.
- Boot failures might occur when booting with a MicroSD card in Legacy mode.
- Changed the resolution of a Redfish SSD wear field to display in percentage.
- The date and time settings are reset after a firmware update.
- The server powers on instead of shutting down when multiple power-on requests are sent.

SECURITY FIXES:

For the latest security bulletins and vulnerabilities addressed in this version, please visit:
https://support.hpe.com/hpesc/public/home

Security best practices:

Please refer to the HPE Integrated Lights-Out Security Technology Brief for the latest on security best practices at:
http://www.hpe.com/support/iLO4_security_en

Enhancements

This version adds support for the following features and enhancements:

- IPMI/DCMI over LAN access is disabled by default on new servers with iLO 4 2.60.
- IPMI/DCMI over LAN access is disabled after you reset iLO 4 2.60 to the factory default settings.
- Each time iLO starts, it backs up the iLO configuration to the nonvolatile flash memory (NAND). If the SRAM is erased, the

configuration is automatically restored.
- Improved Active Health System logging efficiency to prolong the NAND lifespan.
- Added iLO health status to the Overview page. If the status is Degraded, this value is also displayed on the Login page.
- Added an SNMP trap for a power fault condition on Gen8 servers.
- Added the list of open source licenses to the login page.
- Added a Format Embedded Flash and reset iLO button to the Diagnostics page. When directed by Hewlett Packard Enterprise support, you can use this feature to recover Active Health System functionality.
- Re-signed the Java IRC to extend the certificate expiration date.
- Re-signed the .NET IRC to extend the certificate expiration date.
  - With this enhancement, the .NET IRC requires version 4.5.1 or later of the .NET Framework.
- Added the ability to remove a SSL certificate and regenerate the iLO self-signed certificate.
  - Note: HPE recommends using a CA signed certificate.

Online ROM Flash Component for Linux - HPE Integrated Lights-Out 5
Version: 1.30 **(Critical)**
Filename: CP034170.scexe; RPMS/x86_64/firmware-ilo5-1.30-1.1.x86_64.compsig; RPMS/x86_64/firmware-ilo5-1.30-1.1.x86_64.rpm

Important Note!

Install this update to take advantage of significant improvements to the write algorithm for the embedded 4 GB non-volatile flash memory (also known as the NAND). These improvements increase the NAND lifespan.

IPv6 network communications - Dedicated network connection only
Supported Networking Features
IPv6 Static Address Assignment
IPv6 SLAAC Address Assignment
IPv6 Static Route Assignment
IPv6 Static Default Gateway Entry
DHCPv6 Stateful Address Assignment
DHCPv6 Stateless DNS, Domain Name, and NTP Configuration
Integrated Remote Console
OA Single Sign-On
HP-SIM Single Sign-On
Web Server
SSH Server
SNTP Client
DDNS Client
RIBCL over IPv6
SNMP
AlertMail
Remote Syslog
WinDBG Support
CPQLOCFG/HPLOMIG over an IPv6 connection
Scriptable Virtual Media
CLI/RIBCL Key Import over IPv6
Authentication using LDAP and Kerberos over IPv6
iLO Federation
Networking Features not supported by IPv6 in this release
IPv6 Over Shared Network Port Connections
IPMI
NETBIOS-WINS
Enterprise Secure Key Manager (ESKM) Support
Embedded Remote Support (ERS)

Prerequisites

Hewlett Packard Enterprise recommends the following or greater versions of iLO utilities for best performance:

- RESTful Interface Tool (iLOREST) 2.3

HPQLOCFG v5.2
Lights-Out XML Scripting Sample bundle 5.10.0
HPONCFG Windows 5.2.0
HPONCFG Linux 5.3.0
LOCFG v5.10.0
HPLOMIG 5.2.0

NOTE: Updated utilities and system libraries are required to support the iLO HighSecurity, FIPS, and CNSA security states. The HPONCFG Windows utility does not currently support the CNSA security state.

Fixes

The following issues are resolved in this version:

Compute modules do not power on after restoring power to Frame.

- When you use iLO Virtual Media to install an operating system, installation might fail when iLO is configured to use the Shared Network Port.
- In rare cases, a server runs out of available SSH sessions because the sessions are not reclaimed when a client disconnects.
- iLO 5 unexpectedly restored itself to the factory default settings when a user did not initiate the process.
- When Auto Power-On is set to Always Power On or Restore Last Power State, the server might not power on after a cold reset.
- iLO cannot display the HP Ethernet 1Gb 4-port 331i Adapter MAC address.
- NVMe drive model numbers are incorrect or inconsistent.
- Clearing the oemHPE_usercntxt## from the command line clears the value, even though error messages might be displayed.
- Fixed Single Sign-On when in CNSA mode.
- Added support for RSA-PSS certificate signatures.

For the latest security bulletins and vulnerabilities, please visit:
https://support.hpe.com/hpesc/public/home

Please refer to the HPE Integrated Lights-Out 5 Security Technology Brief for the latest on security best practices at:
http://www.hpe.com/support/ilo5-security-en

Enhancements

This version adds support for the following features and enhancements:

- Added support for new platforms:
  - HPE ProLiant ML10 Gen10 Server
- Improved HTML5 IRC performance, including:
  - Added virtual keys to improve the ability to send keyboard actions to the server.
  - Added the ability to configure the keyboard layout in the HTML5 IRC
  - Added Virtual Media support for local ISO and IMG files.
- Firmware and software update enhancements:
  - iLO users can now view, create, and delete maintenance windows.
  - A new check box allows users to clear the installation queue when initiating an install set.
  - Updated the iLO RESTful API and iLO web interface to report when a reboot is required after an installation task completes.
- Each time iLO starts, it backs up the iLO configuration to the nonvolatile flash memory (NAND). If the SRAM is erased, the configuration is automatically restored.
- Added iLO web interface support for Density Optimized Drive Zoning features on supported HPE Apollo products.
- AlertMail now supports SSL (TLS) for secure email.
- AlertMail now supports external SMTP mail servers.
- Added an SNMP trap for when all host NICs are down.
- Updated to OpenSSL-1.0.2u-fips-2.0.16.
- Added the list of open source licenses to the login page.
- Added an SNMP trap for when iLO is reset by IPMI watchdog.
- Added Intelligent System Tuning features to the iLO web interface. From the iLO web interface, you can view the configured settings, configure Jitter Smoothing, and launch Intelligent Provisioning to configure Workload Matching and Core Boosting.
- Improved Active Health System logging efficiency to prolong the NAND lifespan.
- Added iLO health status to the Overview page. If the status is Degraded, this value is also displayed on the Login page.
- Re-signed the Java IRC to extend the certificate expiration date.
- Re-signed the .NET IRC to extend the certificate expiration date.
  - With this enhancement, the .NET IRC requires version 4.5.1 or later of the .NET Framework.
- Added the ability to remove an SSL certificate and regenerate the iLO self-signed certificate.
  - Hewlett Packard Enterprise recommends that you install a CA signed certificate.

Online ROM Flash Component for VMware ESXi - HPE Integrated Lights-Out 4
Version: 2.60 **(Critical)**
Filename: CP033804.compsig; CP033804.zip

Important Note!

Install this update to take advantage of significant improvements to the write algorithm for the embedded 4 GB non-volatile flash memory (also known as the NAND). These improvements increase the NAND lifespan.

IPv6 network communications - Dedicated network connection only
Supported Networking Features
IPv6 Static Address Assignment
IPv6 SLAAC Address Assignment
IPv6 Static Route Assignment
IPv6 Static Default Gateway Entry
DHCPv6 Stateful Address Assignment
DHCPv6 Stateless DNS, Domain Name, and NTP Configuration
Integrated Remote Console
OA Single Sign-On
HP-SIM Single Sign-On
Web Server
SSH Server
SNTP Client
DDNS Client
RIBCL over IPv6
SNMP
AlertMail

Remote Syslog
WinDBG Support
CPQLOCFG/HPLOMIG over an IPv6 connection
Scriptable Virtual Media
CLI/RIBCL Key Import over IPv6
Authentication using LDAP and Kerberos over IPv6
iLO Federation

Networking Features not supported by IPv6 in this release

IPv6 Over Shared Network Port Connections
IPMI
NETBIOS-WINS
Enterprise Secure Key Manager (ESKM) Support
Embedded Remote Support (ERS)

Prerequisites

Hewlett Packard Enterprise recommends upgrading to the minimum versions of the iLO utilities:

- RESTful Interface Tool (iLOREST) 2.3
- HPQLOCFG v5.2
- Lights-Out XML Scripting Sample bundle 5.10.0
- HPONCFG Windows 5.2.0
- HPONCFG Linux 5.3.0
- LOCFG v5.10.0
- HPLOMIG 5.2.0

Fixes

The following issues are resolved in this version:

- iLO 4 unexpectedly restored itself to factory default settings when an user did not initiate the process.
- When Auto Power-On is set to Always Power On to Restore Last Power State, the server might not power on after a cold reset.
- False nonvolatile flash memory (NAND) test failures might occur after a firmware upgrade.
- Incorrect RAM and Storage values are displayed on the HPE OneView for VMware vCenter tab.
- Remote Support disk events include the text "Not Available" for the variables when data is missing.
- Some Power Supply information is missing from the iLO web interface.
- iLO displays Failed status instead of Disabled status when the Smart Array Cache Module battery is disconnected.
- An iLO SSH port disconnection issue was observed after more than two days of continuous operation.
- Values do not move up when the preceding entries in the Directory User Context fields are cleared.
- Boot failures might occur when booting with a MicroSD card in Legacy mode.
- Changed the resolution of a Redfish SSD wear field to display in percentage.
- The date and time settings are reset after a firmware update.
- The server powers on instead of shutting down when multiple power-on requests are sent.

SECURITY FIXES:

For the latest security bulletins and vulnerabilities addressed in this version, please visit:
https://support.hpe.com/hpesc/public/home

Security best practices:

Please refer to the HPE Integrated Lights-Out Security Technology Brief for the latest on security best practices at:
http://www.hpe.com/support/iLO4_security_en

Enhancements

This version adds support for the following features and enhancements:

- IPMI/DCMI over LAN access is disabled by default on new servers with iLO 4 2.60.
- IPMI/DCMI over LAN access is disabled after you reset iLO 4 2.60 to the factory default settings.
- Each time iLO starts, it backs up the iLO configuration to the nonvolatile flash memory (NAND). If the SRAM is erased, the configuration is automatically restored.
- Improved Active Health System logging efficiency to prolong the NAND lifespan.
- Added iLO health status to the Overview page. If the status is Degraded, this value is also displayed on the Login page.
- Added an SNMP trap for a power fault condition on Gen8 servers.
- Added the list of open source licenses to the login page.
- Added a Format Embedded Flash and reset iLO button to the Diagnostics page. When directed by Hewlett Packard Enterprise support, you can use this feature to recover Active Health System functionality.
- Re-signed the Java IRC to extend the certificate expiration date.
- Re-signed the .NET IRC to extend the certificate expiration date.
  - With this enhancement, the .NET IRC requires version 4.5.1 or later of the .NET Framework.
- Added the ability to remove a SSL certificate and regenerate the iLO self-signed certificate.
  - Note: HPE recommends using a CA signed certificate.

Filename: cp033803.exe

Important Note!

Install this update to take advantage of significant improvements to the write algorithm for the embedded 4 GB non-volatile flash memory (also known as the NAND). These improvements increase the NAND lifespan.

IPv6 network communications - Dedicated network connection only

Supported Networking Features

- IPv6 Static Address Assignment
- IPv6 SLAAC Address Assignment
- IPv6 Static Route Assignment
- IPv6 Static Default Gateway Entry
- DHCPv6 Stateful Address Assignment
- DHCPv6 Stateless DNS, Domain Name, and NTP Configuration
- Integrated Remote Console
- OA Single Sign-On
- HP-SIM Single Sign-On
- Web Server
- SSH Server
- SNTP Client
- DDNS Client
- RIBCL over IPv6
- SNMP
- AlertMail
- Remote Syslog
- WinDBG Support
- CPQLOCFG/HPLOMIG over an IPv6 connection
- Scriptable Virtual Media
- CLI/RIBCL Key Import over IPv6
- Authentication using LDAP and Kerberos over IPv6
- iLO Federation

Networking Features not supported by IPv6 in this release

- IPv6 Over Shared Network Port Connections
- IPMI
- NETBIOS-WINS
- Enterprise Secure Key Manager (ESKM) Support
- Embedded Remote Support (ERS)

Prerequisites

Hewlett Packard Enterprise recommends upgrading to the minimum versions of the iLO utilities:

- RESTful Interface Tool (iLOREST) 2.3
- HPQLOCFG v5.2
- Lights-Out XML Scripting Sample bundle 5.10.0
- HPONCFG Windows 5.2.0
- HPONCFG Linux 5.3.0
- LOCFG v5.10.0
- HPLOMIG 5.2.0

Fixes

The following issues are resolved in this version:

- iLO 4 unexpectedly restored itself to factory default settings when an user did not initiate the process.
- When Auto Power-On is set to Always Power On to Restore Last Power State, the server might not power on after a cold reset.
- False nonvolatile flash memory (NAND) test failures might occur after a firmware upgrade.
- Incorrect RAM and Storage values are displayed on the HPE OneView for VMware vCenter tab.
- Remote Support disk events include the text "Not Available" for the variables when data is missing.
- Some Power Supply information is missing from the iLO web interface.
- iLO displays Failed status instead of Disabled status when the Smart Array Cache Module battery is disconnected.
- An iLO SSH port disconnection issue was observed after more than two days of continuous operation.
- Values do not move up when the preceding entries in the Directory User Context fields are cleared.
- Boot failures might occur when booting with a MicroSD card in Legacy mode.
- Changed the resolution of a Redfish SSD wear field to display in percentage.
- The date and time settings are reset after a firmware update.
- The server powers on instead of shutting down when multiple power-on requests are sent.

SECURITY FIXES:

For the latest security bulletins and vulnerabilities addressed in this version, please visit:
https://support.hpe.com/hpesc/public/home

Security best practices:

Please refer to the HPE Integrated Lights-Out Security Technology Brief for the latest on security best practices at:
http://www.hpe.com/support/iLO4_security_en

Enhancements

This version adds support for the following features and enhancements:

- IPMI/DCMI over LAN access is disabled by default on new servers with iLO 4 2.60.
- IPMI/DCMI over LAN access is disabled after you reset iLO 4 2.60 to the factory default settings.
- Each time iLO starts, it backs up the iLO configuration to the nonvolatile flash memory (NAND). If the SRAM is erased, the configuration is automatically restored.
- Improved Active Health System logging efficiency to prolong the NAND lifespan.
- Added iLO health status to the Overview page. If the status is Degraded, this value is also displayed on the Login page.
- Added an SNMP trap for a power fault condition on Gen8 servers.
- Added the list of open source licenses to the login page.
- Added a Format Embedded Flash and reset iLO button to the Diagnostics page. When directed by Hewlett Packard Enterprise support, you can use this feature to recover Active Health System functionality.
- Re-signed the Java IRC to extend the certificate expiration date.
- Re-signed the .NET IRC to extend the certificate expiration date.
  - With this enhancement, the .NET IRC requires version 4.5.1 or later of the .NET Framework.
- Added the ability to remove a SSL certificate and regenerate the iLO self-signed certificate.
  - Note: HPE recommends using a CA signed certificate.

Online ROM Flash Component for Windows x64 - HPE Integrated Lights-Out 5
Version: 1.30 **(Critical)**
Filename: cp034171.compsig; cp034171.exe

Important Note!

Install this update to take advantage of significant improvements to the write algorithm for the embedded 4 GB non-volatile flash memory (also known as the NAND). These improvements increase the NAND lifespan.

IPv6 network communications - Dedicated network connection only
Supported Networking Features
IPv6 Static Address Assignment
IPv6 SLAAC Address Assignment
IPv6 Static Route Assignment
IPv6 Static Default Gateway Entry
DHCPv6 Stateful Address Assignment
DHCPv6 Stateless DNS, Domain Name, and NTP Configuration
Integrated Remote Console
OA Single Sign-On
HP-SIM Single Sign-On
Web Server
SSH Server
SNTP Client
DDNS Client
RIBCL over IPv6
SNMP
AlertMail
Remote Syslog
WinDBG Support
CPQLOCFG/HPLOMIG over an IPv6 connection
Scriptable Virtual Media
CLI/RIBCL Key Import over IPv6
Authentication using LDAP and Kerberos over IPv6
iLO Federation
Networking Features not supported by IPv6 in this release
IPv6 Over Shared Network Port Connections
IPMI
NETBIOS-WINS
Enterprise Secure Key Manager (ESKM) Support
Embedded Remote Support (ERS)

Prerequisites

Hewlett Packard Enterprise recommends the following or greater versions of iLO utilities for best performance:

- RESTful Interface Tool (iLOREST) 2.3
- HPQLOCFG v5.2
- Lights-Out XML Scripting Sample bundle 5.10.0
- HPONCFG Windows 5.2.0
- HPONCFG Linux 5.3.0
- LOCFG v5.10.0
- HPLOMIG 5.2.0

NOTE: Updated utilities and system libraries are required to support the iLO HighSecurity, FIPS, and CNSA security states. The HPONCFG Windows utility

does not currently support the CNSA security state.

Fixes

The following issues are resolved in this version:

- Compute modules do not power on after restoring power to Frame.
- When you use iLO Virtual Media to install an operating system, installation might fail when iLO is configured to use the Shared Network Port.
- In rare cases, a server runs out of available SSH sessions because the sessions are not reclaimed when a client disconnects.
- iLO 5 unexpectedly restored itself to the factory default settings when a user did not initiate the process.
- When Auto Power-On is set to Always Power On or Restore Last Power State, the server might not power on after a cold reset.
- iLO cannot display the HP Ethernet 1Gb 4-port 331i Adapter MAC address.
- NVMe drive model numbers are incorrect or inconsistent.
- Clearing the oemHPE_usercntxt## from the command line clears the value, even though error messages might be displayed.
- Fixed Single Sign-On when in CNSA mode.
- Added support for RSA-PSS certificate signatures.

For the latest security bulletins and vulnerabilities, please visit:
https://support.hpe.com/hpesc/public/home

Please refer to the HPE Integrated Lights-Out 5 Security Technology Brief for the latest on security best practices at:
http://www.hpe.com/support/ilo5-security-en

Enhancements

This version adds support for the following features and enhancements:

- Added support for new platforms:
  - HPE ProLiant ML10 Gen10 Server
- Improved HTML5 IRC performance, including:
  - Added virtual keys to improve the ability to send keyboard actions to the server.
  - Added the ability to configure the keyboard layout in the HTML5 IRC
  - Added Virtual Media support for local ISO and IMG files.
- Firmware and software update enhancements:
  - iLO users can now view, create, and delete maintenance windows.
  - A new check box allows users to clear the installation queue when initiating an install set.
  - Updated the iLO RESTful API and iLO web interface to report when a reboot is required after an installation task completes.
- Each time iLO starts, it backs up the iLO configuration to the nonvolatile flash memory (NAND). If the SRAM is erased, the configuration is automatically restored.
- Added iLO web interface support for Density Optimized Drive Zoning features on supported HPE Apollo products.
- AlertMail now supports SSL (TLS) for secure email.
- AlertMail now supports external SMTP mail servers.
- Added an SNMP trap for when all host NICs are down.
- Updated to OpenSSL-1.0.2u-fips-2.0.16.
- Added the list of open source licenses to the login page.
- Added an SNMP trap for when iLO is reset by IPMI watchdog.
- Added Intelligent System Tuning features to the iLO web interface. From the iLO web interface, you can view the configured settings, configure Jitter Smoothing, and launch Intelligent Provisioning to configure Workload Matching and Core Boosting.
- Improved Active Health System logging efficiency to prolong the NAND lifespan.
- Added iLO health status to the Overview page. If the status is Degraded, this value is also displayed on the Login page.
- Re-signed the Java IRC to extend the certificate expiration date.
- Re-signed the .NET IRC to extend the certificate expiration date.
  - With this enhancement, the .NET IRC requires version 4.5.1 or later of the .NET Framework.
- Added the ability to remove an SSL certificate and regenerate the iLO self-signed certificate.
  - Hewlett Packard Enterprise recommends that you install a CA signed certificate.

Firmware - Network Top

HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Linux x86_64
Version: 1.3.10 **(Optional)**
Filename: firmware-nic-bcm-nxe-1.3.10-1.1.x86_64.compsig; firmware-nic-bcm-nxe-1.3.10-1.1.x86_64.rpm

Important Note!

HPE recommends the *HPE Broadcom NetXtreme-E Drivers for Linux*, versions 1.9.1-212.0.99.0 or later, for use with this firmware.

Prerequisites

This package requires the appropriate driver for your network adapter be installed and all Ethernet ports brought up (*ifup ethX* or *ifconfig ethX up*) before firmware can be updated.

Fixes

This product corrects a link flap seen when updating NIC firmware.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Windows Server x64 Editions
Version: 5.1.3.0 **(Optional)**
Filename: cp034397.compsig; cp034397.exe

Important Note!

HPE recommends *HPE Broadcom NetXtreme-E Driver for Windows*, versions 212.0.89.0 or later, for use with this firmware.

Prerequisites

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

Fixes

This product corrects a link flap seen when updating NIC firmware.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 535FLR-T Adapter
- HPE Ethernet 10Gb 2-port 535T Adapter
- HPE Ethernet 10/25Gb 2-port 631FLR-SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 631SFP28 Adapter

HPE Broadcom NX1 Online Firmware Upgrade Utility for Linux x86_64
Version: 2.21.3 **(Optional)**
Filename: firmware-nic-broadcom-2.21.3-1.1.x86_64.compsig; firmware-nic-broadcom-2.21.3-1.1.x86_64.rpm

Important Note!

HPE recommends *HPE Broadcom tg3 Ethernet Drivers*, versions 3.137w-1 or later, for use with this firmware.

Prerequisites

This package requires the appropriate driver for your network adapter be installed and all Ethernet ports brought up (*ifup ethX* or *ifconfig ethX up*) before firmware can be updated.

Fixes

This product addresses an issue where the NIC Serial Number for the HPE Ethernet 1Gb 4-port 331FLR Adapter is not displayed in AHS.

The firmware in this product addresses an issue where the "Reboot Required" icon is not highlighted after a NIC firmware update (via System Utilities->Embedded Application->Firmware Update) completes.

Supported Devices and Features

This product supports the following network adapters:

- HP Ethernet 1Gb 2-port 330i Adapter (22BD)
- HP Ethernet 1Gb 4-port 331i Adapter (22BE)
- HPE Ethernet 1Gb 4-port 331FLR Adapter
- HPE Ethernet 1Gb 4-port 331T Adapter
- HP Ethernet 1Gb 2-port 332i Adapter (2133)
- HP Ethernet 1Gb 2-port 332i Adapter (22E8)
- HPE Ethernet 1Gb 2-port 332T Adapter

HPE Broadcom NX1 Online Firmware Upgrade Utility for VMware
Version: 1.21.3 **(Optional)**
Filename: CP034765.compsig; CP034765.zip

Important Note!

HPE recommends *HP Broadcom tg3 Ethernet Drivers for VMware*, versions 2015.10.01 or later, for use with this firmware.

This software package contains combo image v20.12.41 with the following firmware versions:

NIC	Boot Code Version	PXE Version	NCSI Version	UEFI Version	CCM Version
HP Ethernet 1Gb 2-port 330i Adapter (22BD)	2.10	20.6.50	1.4.22	20.12.2	212.0.92.0
HP Ethernet 1Gb 4-port 331i Adapter (22BE) HP Ethernet 1Gb 4-port 331FLR Adapter HP Ethernet 1Gb 4-port 331T Adapter	1.46	20.6.50	1.4.22	20.12.2	212.0.92.0
HP Ethernet 1Gb 2-port 332i Adapter (2133)	1.39	20.6.50	1.4.22	n/a	212.0.92.0
HP Ethernet 1Gb 2-port 332i Adapter (22E8) HP Ethernet 1Gb 2-port 332T Adapter	1.39	20.6.50	1.4.22	20.12.2	212.0.92.0

Prerequisites

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

Fixes

This product addresses an issue where the NIC Serial Number for the HPE Ethernet 1Gb 4-port 331FLR Adapter is not displayed in AHS.

The firmware in this product addresses an issue where the "Reboot Required" icon is not highlighted after a NIC firmware update (via System Utilities->Embedded Application->Firmware Update) completes.

Supported Devices and Features

This product supports the following network adapters:

- HP Ethernet 1Gb 2-port 330i Adapter (22BD)
- HP Ethernet 1Gb 4-port 331i Adapter (22BE)
- HPE Ethernet 1Gb 4-port 331FLR Adapter
- HPE Ethernet 1Gb 4-port 331T Adapter
- HP Ethernet 1Gb 2-port 332i Adapter (2133)
- HP Ethernet 1Gb 2-port 332i Adapter (22E8)
- HPE Ethernet 1Gb 2-port 332T Adapter

HPE Broadcom NX1 Online Firmware Upgrade Utility for Windows Server x64 Editions
Version: 5.1.3.0 **(Optional)**
Filename: cp034766.compsig; cp034766.exe

Important Note!

HPE recommends *HPE Broadcom 1Gb Driver for Windows Server x64 Editions*, version 212.0.0.0 or later, for use with this firmware.

Prerequisites

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

Fixes

This product addresses an issue where the NIC Serial Number for the HPE Ethernet 1Gb 4-port 331FLR Adapter is not displayed in AHS.

The firmware in this product addresses an issue where the "Reboot Required" icon is not highlighted after a NIC firmware update (via System Utilities->Embedded Application->Firmware Update) completes.

Supported Devices and Features

This product supports the following network adapters:

- HP Ethernet 1Gb 2-port 330i Adapter (22BD)
- HP Ethernet 1Gb 4-port 331i Adapter (22BE)
- HPE Ethernet 1Gb 4-port 331FLR Adapter
- HPE Ethernet 1Gb 4-port 331T Adapter
- HP Ethernet 1Gb 2-port 332i Adapter (2133)
- HP Ethernet 1Gb 2-port 332i Adapter (22E8)
- HPE Ethernet 1Gb 2-port 332T Adapter

HPE Firmware Flash for Emulex Converged Network Adapters for Linux (x64)
Version: 2018.06.01 **(Recommended)**
Filename: RPMS/x86_64/firmware-cna-emulex-2018.06.01-1.16.x86_64.compsig; RPMS/x86_64/firmware-cna-emulex-2018.06.01-1.16.x86_64.rpm

Important Note!

Release Notes:

HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Firmware updates may be accomplished using the inbox or Out of Box (OOB) drivers. Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The OOB NIC driver is available on the Service Pack for ProLiant (SPP) which is available at http://www.hpe.com/servers/spp/download.

Additional requirements:

The target environment must have the libsysfs or sysfsutils package installed prior to the installation of the firmware update kit. If not already present, the libsysfs or sysfsutils package can be obtained from the operating system installation media.

Environment must have 32-bit netlink library (libnl.so) installed for component to be able to discover Emulex HBAs/CNAs
Environment must be running the syslog daemon for the flash engine to run

Note: To enable the FCoE/iSCSI protocol on devices that support it, please install the appropriate Emulex FCoE/iSCSI driver. The FCoE protocol also requires the HPE Emulex FCoE Enablement Kit be installed. The drivers and enablement kit are also available on the Service Pack for ProLiant (SPP) which is available at http://www.hpe.com/servers/spp/download.

The Enablement Kit requires that the target environment have the libHBAAPI package installed from your OS installation media.

Install the FCoE Driver Kit, reboot, and then install the Enablement Kit.

Fixes

Fixed the following:

- Add a check for zero capacity LUNs (Logical Units) and avoid creating device path for them.
- HP StoreFabric CN1200E Dual Port Converged Network Adapter FCoE function only show "Slot 3 Port 3:CN1200E Function 2-FCoE"

Enhancements

We have separate components to update fibre channel and converged network adapters. This is a converged network adapter update component.

Updated CNA (XE100 series) firmware

Firmware

Contains:
CNA (XE100 series) firmware 12.0.1110.11

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter

- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Firmware Flash for Emulex Converged Network Adapters for VMware vSphere 6.5
Version: 2018.06.01 **(Recommended)**
Filename: CP034213.compsig; CP034213.zip

Important Note!

Release Notes:

HPE StoreFabric Emulex Adapter Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Fixes

Fixed the following:

- Add a check for zero capacity LUNs (Logical Units) and avoid creating device path for them.
- HP StoreFabric CN1200E Dual Port Converged Network Adapter FCoE function only show "Slot 3 Port 3:CN1200E Function 2-FCoE"

Enhancements

We have separate components to update fibre channel and converged network adapters. This is a Converge Network Adapter update component.

Updated CNA (XE100 series) firmware

Firmware

Contains:

CNA (XE100 series) firmware 12.0.1110.11

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Firmware Flash for Emulex Converged Network Adapters for VMware vSphere 6.0
Version: 2018.06.01 **(Recommended)**
Filename: CP034212.compsig; CP034212.zip

Important Note!

Release Notes:

HPE StoreFabric Emulex Adapter Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Fixes

Fixed the following:

- Add a check for zero capacity LUNs (Logical Units) and avoid creating device path for them.
- HP StoreFabric CN1200E Dual Port Converged Network Adapter FCoE function only show "Slot 3 Port 3:CN1200E Function 2-FCoE"

Enhancements

We have separate components to update fibre channel and converged network adapters. This is a Converge Network Adapter update component.

Updated CNA (XE100 series) firmware

Firmware

Contains:

CNA (XE100 series) firmware 12.0.1110.11

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Firmware Flash for Emulex Converged Network Adapters for Windows (x64)
Version: 2018.06.01 **(Recommended)**
Filename: cp034215.compsig; cp034215.exe

Important Note!

Release Notes:

HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Firmware updates may be accomplished using the inbox or Out of Box (OOB) drivers. Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied Emulex NIC driver must be installed prior to this firmware component being identified by SUM for deployment. The latest driver is available on the HPE.com website at http://www.hpe.com/.

The FCoE/iSCSI OOB driver and FCoE enablement kit are available on the Service Pack for ProLiant (SPP) which is available at http://www.hpe.com/servers/spp/download.

Fixes

Fixed the following:

- Add a check for zero capacity LUNs (Logical Units) and avoid creating device path for them.
- HP StoreFabric CN1200E Dual Port Converged Network Adapter FCoE function only show "Slot 3 Port 3:CN1200E Function 2-FCoE"

Enhancements

We have separate components to update fibre channel and converged network adapters. This is a Converge Network Adapter update component.

Updated CNA (XE100 series) firmware

Firmware

Contains:
CNA (XE100 series) firmware 12.0.1110.11

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Intel Online Firmware Upgrade Utility for Linux x86_64
Version: 1.15.9 **(Optional)**
Filename: firmware-nic-intel-1.15.9-1.1.x86_64.compsig; firmware-nic-intel-1.15.9-1.1.x86_64.rpm

Important Note!

HPE recommends at least one of the following drivers, as appropriate for your device, for use with this firmware:

- HPE Intel igb Drivers for Linux, versions 5.3.5.15 or later
- HPE Intel ixgbe Drivers for Linux , versions 5.3.5.1 or later
- HPE Intel i40e Drivers for Linux, versions 2.4.6 or later

Prerequisites

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

Fixes

This product addresses a NIC VLAN ID issue seen in the NIC Human Interface Infrastructure (HII) menu when operating in UEFI mode.
This product addresses a teaming issue where the HPE Ethernet 10Gb 2-port 561T Adapter still shows connected on the switch after the NIC has been disabled.
This product addresses a link issue and a PXE issue seen with the HPE Ethernet 10Gb 2-port 560FLB Adapter.
This product addresses a WOL issue seen with the HPE Ethernet 1Gb 4-port 366T Adapter.

Supported Devices and Features

This package supports the following network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HP Ethernet 1Gb 4-port 366i Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter
- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 563i Adapter
- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter

HPE Intel Online Firmware Upgrade Utility for VMware
Version: 3.7.8 **(Optional)**
Filename: CP034064.compsig; CP034064.zip

Important Note!

HPE recommends at least one of the following drivers, as appropriate for your device, for use with this firmware:

- *HPE Intel igbn Drivers for VMware*, versions 2018.06.04
- *HPE Intel ixgben Drivers for VMware*, versions 2018.06.04
- *HPE Intel i40en Drivers for VMware*, versions 2018.06.04

This software package contains the following firmware versions for the below listed supported nework adapters:

NIC	EEPROM/NVM Version	OROM Version	Single NVM Version
HP Ethernet 1Gb 2-port 361i Adapter	80000CD5	1.1904.0	N/A
HP Ethernet 1Gb 2-port 361T Adapter	80000F91	1.1904.0	N/A
HP Ethernet 1Gb 2-port 363i Adapter	80000D00	1.1904.0	N/A
HP Ethernet 1Gb 1-port 364i Adapter	80000BEE	1.1904.0	N/A
HP Ethernet 1Gb 4-port 366i Adapter	80000E24	1.1904.0	N/A
HPE Ethernet 1Gb 4-port 366i Communication Board	80000EBF	1.1904.0	N/A
HP Ethernet 1Gb 4-port 366FLR Adapter	80000F44	1.1904.0	N/A
HP Ethernet 1Gb 4-port 366M Adapter	80000DA9	1.1904.0	N/A
HP Ethernet 1Gb 4-port 366T Adapter	80000E81	1.1904.0	N/A
HPE Ethernet 1Gb 2-port 368i Adapter	80001111	1.1904.0	N/A
HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter	80001110	1.1904.0	N/A
HPE Ethernet 1Gb 4-port 369i Adapter	80001112	1.1904.0	N/A
HP Ethernet 10Gb 2-port 560FLB Adapter	800008F0	1.1904.0	N/A
HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter	80000838	1.1904.0	N/A
HP Ethernet 10Gb 2-port 560M Adapter	8000083D	1.1904.0	N/A
HPE Ethernet 10Gb 2-port 560SFP+ Adapter	80000835	1.1904.0	N/A
HP Ethernet 10Gb 2-port 561FLR-T Adapter	800005B6	1.1904.0	N/A
HP Ethernet 10Gb 2-port 561T Adapter	80000636	1.1904.0	N/A
HPE Ethernet 10Gb 2-port 568i Adapter	80001113	1.1904.0	N/A
HPE Ethernet 10Gb 2-port 568FLR-MMSFP+			

Adapter	80001110	1.1904.0	N/A
HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter	80001110	1.1904.0	N/A
HPE Ethernet 10Gb 2-port 563i Adapter	800035C0	1.1375.0	N/A
HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter	800038C9	1.1904.0	10.3.5
HPE Ethernet 10Gb 2-port 562FLR-T Adapter	80000BF1	1.1904.0	10.3.5
HPE Ethernet 10Gb 2-port 562SFP+ Adapter	800038C8	1.1904.0	10.3.5
HPE Ethernet 10Gb 2-port 562T Adapter	80000BF0	1.1904.0	10.3.5

The combo image v1.1904.0 includes: Boot Agent: 1GbE - v1.5.85, 10GbE - v2.4.16, 40GbE - v1.0.66 & UEFI Drivers: 1GbE - v8.3.10, 10GbE - v6.7.10, 40GbE - v3.0.11

The combo image v1.1375.0 includes: Boot Agent: 1GbE - v1.5.72, 10GbE - v2.3.46, 40GbE - v1.0.21 & UEFI Drivers: 1GbE - v6.9.13, 10GbE - v5.0.20, 40GbE - v1.5.14.

Single NVM Version is new firmware format which represent an unified version in place of the previously used EEPROM/NVM Version or OROM version.

Prerequisites

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

Fixes

This product addresses a NIC VLAN ID issue seen in the NIC Human Interface Infrastructure (HII) menu when operating in UEFI mode.
This product addresses a teaming issue where the HPE Ethernet 10Gb 2-port 561T Adapter still shows connected on the switch after the NIC has been disabled.
This product addresses a link issue and a PXE issue seen with the HPE Ethernet 10Gb 2-port 560FLB Adapter.
This product addresses a WOL issue seen with the HPE Ethernet 1Gb 4-port 366T Adapter.

Supported Devices and Features

This package supports the following network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HP Ethernet 1Gb 4-port 366i Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter
- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 563i Adapter
- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 562T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter

HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Editions
Version: 5.1.3.0 **(Optional)**
Filename: cp034074.compsig; cp034074.exe

Important Note!

HPE recommends at least one of the following, as appropriate for your device, for use with this firmware:

- *HPE Intel E1R Driver for Windows Server 2012*, versions 12.14.8.0 or later
- *HPE Intel E1R Driver for Windows Server 2016*, version 12.15.184.0(B) or later
- *HPE Intel ixn Driver for Windows Server 2012*, versions 3.14.76.0 or later
- *HPE Intel ixn Driver for Windows Server 2016*, version 4.1.74.0 or later
- *HPE Intel ixs Driver for Windows Server 2012 R2*, version 3.14.75.0 or later

- *HPE Intel ixs Driver for Windows Server 2016*, version 4.1.74.0 or later
- *HPE Intel ixt Driver for Windows Server 2012*, versions 3.14.76.0 or later
- *HPE Intel ixt Driver for Windows Server 2016*, version 4.1.74.0 or later
- *HPE Intel i40ea Driver for Windows*, versions 1.8.94.0 or later
- *HPE Intel i40eb Driver for Windows*, versions 1.8.94.0 or later

Prerequisites

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

Fixes

This product addresses a NIC VLAN ID issue seen in the NIC Human Interface Infrastructure (HII) menu when operating in UEFI mode.
This product addresses a teaming issue where the HPE Ethernet 10Gb 2-port 561T Adapter still shows connected on the switch after the NIC has been disabled.
This product addresses a link issue and a PXE issue seen with the HPE Ethernet 10Gb 2-port 560FLB Adapter.
This product addresses a WOL issue seen with the HPE Ethernet 1Gb 4-port 366T Adapter.

Supported Devices and Features

This package supports the following network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 1-port 364i Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HP Ethernet 1Gb 4-port 366i Adapter
- HPE Ethernet 1Gb 4-port 366i Communication Board
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter
- HPE Ethernet 1Gb 2-port 368i Adapter
- HPE Ethernet 1Gb 2-port 368FLR-MMT Adapter
- HPE Ethernet 1Gb 4-port 369i Adapter
- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HPE Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HPE Ethernet 10Gb 2-port 562FLR-T Adapter
- HPE Ethernet 10Gb 2-port 562SFP+ Adapter HPE
- Ethernet 10Gb 2-port 562T Adapter
- HPE Ethernet 10Gb 2-port 563i Adapter
- HPE Ethernet 10Gb 2-port 568i Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMSFP+ Adapter
- HPE Ethernet 10Gb 2-port 568FLR-MMT Adapter

HPE QLogic FastLinQ Online Firmware Upgrade Utility for Linux x86_64
Version: 1.4.24 **(Optional)**
Filename: firmware-nic-qlogic-flq-1.4.24-1.1.x86_64.compsig; firmware-nic-qlogic-flq-1.4.24-1.1.x86_64.rpm

Important Note!

HPE recommends *HPE QLogic FastLinQ 10/25/50GbE Drivers for Linux,* versions 8.33.17.0-1 or later, for use with the firmware in this product.

Prerequisites

This package requires the appropriate driver for your network adapter be installed and all Ethernet ports brought up (*ifup ethX* or *ifconfig ethX up*) before firmware can be updated.

Fixes

- This product corrects an issue where booting to Preboot eXecution Environment (PXE) may not work after applying the OneView server profile when the System ROM is set to 'Legacy BIOS Mode'.
- This product addresses an issue where the FCoE boot parameters cannot be configured in the adapter's configuration menu (under 'System Utilities'->'System Configuration' menu) when OneView profile with connections set to 'manually managed' is applied to the system.
- This product corrects an issue where certain settings/changes (CHAP, boot mode etc) in the OneView server profile are not reflected in the adapters' configuration menu (under 'System Utilities'->'System Configuration' menu) after applying the OneView server profile.
- This product corrects an issue where the virtual World Wide Port Name(WWPN)/World Wide Node Name(WWNN) are not programmed properly when applying the OneView server profile.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter
- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter

---

HPE QLogic FastLinQ Online Firmware Upgrade Utility for VMware
Version: 4.6.24 **(Optional)**
Filename: CP033812.compsig; CP033812.zip

Important Note!

HPE recommends *HPE QLogic FastLinQ 10/25/50GbE Multifunction Drivers for VMware*, versions 2018.06.04 or later, for use with this firmware.

This software package contains the following firmware versions:

NIC	Boot Code (MFW) Version	UEFI Version	PXE Version	Combo Image Version
HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter	8.35.3.0	4.1.4.25	2.0.17	8.35.09
HPE Synergy 6810C 25/50Gb Ethernet Adapter				
HPE Ethernet 10Gb 2-port 521T Adapter	8.35.3.0	4.1.4.25	2.0.17	8.35.09
HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter				
HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter				

Prerequisites

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

Fixes

- This product corrects an issue where booting to Preboot eXecution Environment (PXE) may not work after applying the OneView server profile when the System ROM is set to 'Legacy BIOS Mode'.
- This product addresses an issue where the FCoE boot parameters cannot be configured in the adapter's configuration menu (under 'System Utilities'->'System Configuration' menu) when OneView profile with connections set to 'manually managed' is applied to the system.
- This product corrects an issue where certain settings/changes (CHAP, boot mode etc) in the OneView server profile are not reflected in the adapters' configuration menu (under 'System Utilities'->'System Configuration' menu) after applying the OneView server profile.
- This product corrects an issue where the virtual World Wide Port Name(WWPN)/World Wide Node Name(WWNN) are not programmed properly when applying the OneView server profile.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic FastLinQ Online Firmware Upgrade Utility for Windows Server x64 Editions
Version: 5.1.3.0 **(Optional)**
Filename: cp033845.compsig; cp033845.exe

Important Note!

HPE recommends *HPE QLogic FastLinQ 10/25/50GbE Driver for Windows Server x64 Editions*, version 8.33.23.0 or later, for use with the firmware in this product.

Prerequisites

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

Fixes

- This product corrects an issue where booting to Preboot eXecution Environment (PXE) may not work after applying the OneView server profile when the System ROM is set to 'Legacy BIOS Mode'.
- This product addresses an issue where the FCoE boot parameters cannot be configured in the adapter's configuration menu (under 'System Utilities'->'System Configuration' menu) when OneView profile with connections set to 'manually managed' is applied to the system.
- This product corrects an issue where certain settings/changes (CHAP, boot mode etc) in the OneView server profile are not reflected in the adapters' configuration menu (under 'System Utilities'->'System Configuration' menu) after applying the OneView server profile.
- This product corrects an issue where the virtual World Wide Port Name(WWPN)/World Wide Node Name(WWNN) are not programmed properly when applying the OneView server profile.

Supported Devices and Features

This product supports the following network adapters:

- HPE Ethernet 10Gb 2-port 521T Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 621SFP28 Adapter
- HPE Ethernet 10/25Gb 2-port 622FLR-SFP28 Converged Network Adapter
- HPE Synergy 6810C 25/50Gb Ethernet Adapter

HPE QLogic NX2 Online Firmware Upgrade Utility for Linux x86_64
Version: 2.22.15 **(Optional)**
Filename: firmware-nic-qlogic-nx2-2.22.15-1.1.x86_64.compsig; firmware-nic-qlogic-nx2-2.22.15-1.1.x86_64.rpm

Important Note!

HPE recommends *HPE QLogic NX2 10/20GbE Multifunction Drivers for Linux*, versions 7.14.46-1 or later, for use with the firmware in this package.

Prerequisites

This package requires the appropriate driver for your network adapter be installed and all Ethernet ports brought up (*ifup ethX* or *ifconfig ethX up*) before firmware can be updated.

Fixes

This product corrects an issue where users may see an error message when they attempt to restore the adapter's configuration settings to defaults by pressing F7 under the 'System Utilities->System Configuration' menu.

Supported Devices and Features

This product supports the following network adapters:

- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP Ethernet 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Network Adapter

HPE QLogic NX2 Online Firmware Upgrade Utility for VMware
Version: 1.21.15 **(Optional)**
Filename: CP034082.compsig; CP034082.zip

Important Note!

HPE recommends *HPE QLogic NX2 10/20GbE Multifunction Drivers for VMware*, versions 2018.06.04 or later, for use with this firmware.

This software package contains combo image v7.17.19 with the following firmware versions:

	Boot Code	PXE	UEFI	iSCSI	FCoE	CCM	L2

NIC	Version	Version	Version	Version	Version	Version	Version
HP Ethernet 10Gb 2-port 530SFP+ Adapter HP Ethernet 10Gb 2-port 530T Adapter	7.15.24	7.14.13	8.2.9	n/a	n/a	7.14.4	7.12.25
HP Ethernet 10Gb 2-port 533FLR-T Adapter HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter HP FlexFabric 10Gb 2-port 534M Adapter HP FlexFabric 10Gb 2-port 536FLB Adapter HPE FlexFabric 10Gb 4-port 536FLR-T Adapter HP FlexFabric 20Gb 2-port 630FLB Adapter HP FlexFabric 20Gb 2-port 630M Adapter HP StoreFabric CN1100R Dual Port Converged Network Adapter HPE StoreFabric CN1100R-T Converged Network Adapter HPE Synergy 3820C 10/20Gb Converged Network Adapter HPE Synergy 2820C 10Gb Converged Network Adapter	7.15.24	7.14.13	8.2.9	7.14.0	7.14.3	7.14.4	7.12.25

Prerequisites

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

Fixes

This product corrects an issue where users may see an error message when they attempt to restore the adapter's configuration settings to defaults by pressing F7 under the 'System Utilities->System Configuration' menu.

Supported Devices and Features

This product supports the following network adapters:

- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP Ethernet 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Network Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

HPE QLogic NX2 Online Firmware Upgrade Utility for Windows Server x64 Editions
Version: 5.1.3.0 **(Optional)**
Filename: cp034083.compsig; cp034083.exe

Important Note!

HPE recommends *HPE QLogic NX2 10/20GbE Multifunction Drivers for Windows Server x64 Editions*, version 7.13.145.0 or later, for use with this firmware.

Prerequisites

This product requires the appropriate driver for your device and operating system be installed before firmware is updated.

Fixes

This product corrects an issue where users may see an error message when they attempt to restore the adapter's configuration settings to defaults by pressing F7 under the 'System Utilities->System Configuration' menu.

Supported Devices and Features

This product supports the following network adapters:

- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP Ethernet 10Gb 2-port 533FLR-T Adapter

- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE Synergy 2820C 10Gb Converged Network Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

Online Firmware Upgrade Utility (ESXi 6.0) for HPE Mellanox Ethernet only adapters
Version: 1.0.8 **(Recommended)**
Filename: CP034531.compsig; CP034531.zip

Important Note!

Known Issues for FW version 2.42.5000 :

- Enabling/disabling cq_timestamp using mlxconfig is not supported.
- In a card with 2 separate LEDs scheme (a Phy LED and a logic LED) only the Phy LED will lit. Meaning, the orange LES will not be active while the ETH link is in an idle mode.
- In SR-IOV setup, using mlxconfig when the PF is passed through to a VM requires a reboot of the Hypervisor.
- Downgrade to previous GA requires server reboot.Downgrading from v2.30.8000 or later to an earlier version than 2.30.8000 requires server reboot. Reboot the server.
- On ConnectX-3 Ethernet adapter cards, there is a mismatch between the GUID value returned by firmware management tools and that returned by fabric/driver utilities that read the GUID via device firmware (e.g., using ibstat). Mlxburn/flint return 0xffff as GUID while the utilities return a value derived from the MAC address. For all driver/firmware/software purposes, the lattervalue should be used.
- SBR should be asserted for a minimum of 50 milliseconds for the ConnectX®-3 adapters
- On Pilot1 SL230, PCIe link occasionally does not come up at Gen3 speed
- RH6.3 Inbox driver causes kernel panic when SR-IOV is enabled on VPI cards due to driver compatibility issue.
- In advanced steering mode, side band management connectivity may be lost when having more than 8 QP per mcg.
- When SR-IOV is disabled in the system BIOS, a PCI issue is noticed in Ubuntu v12.04.3 with Linux kernel v3.8 which affects NICs of several manufacturers including Mellanox's, preventing them from operating.
- MFT tools might leave the flash semaphore locked if the tool operation is forced stopped. The locked semaphore prevents the firmware from accessing the flash and causes firmware hang.
- Cable Info MAD reports a wrong cable info when usingthe MC2210411-SR4 module
- Gen2 failure at temperature sweep up to 10C/min (for MT27518A1-FDIR-BV only).
- PCIe Gen2 link unstable at temperature sweep of 10C/min for MT27518A1-FDIR-BV
- Bloom filter is currently not supported.
- Firmware downgrade message When downgrading from firmware v2.11.0000 and using MFT 3.0.0-3
- RM#DMFS should not be enabled when working with InfiniBand on MLNX_OFED-2.0.3
- RM#VPD read-only fields are writable.
- Increasing SymbolErrorCounter When working in VPI mode with port1 FDR and port2 40G, error counters misbehave and increase rapidly
- Setting the device to 128Byte CQ/EQ stride will cause misbehavior of sideband management resulting in communication loss.
- CQ and EQ cannot be configured to different stride sizes.
- ConnectX-3 Pro VF device ID is presented the same as ConnectX-3 VF device ID due to driver limitations.
- RSOD while running PXE (legacy) on G9 servers. This occurs only when PXE boot fails and BIOS boots from HDD. Currently it is pending BIOS fix.
- Changing port protocol from ETH to IB on port with NCSI/IPMI enabled while the port is connected to ETH switch is not supported.
- RDP over IPv6 is currently not functional.
- Sniffer QP cannot be removed from the regular rule after adding the QP with insertion scheme equals to "push to that rule"
- Since only a single Boot Entry Vector (BEV) per PCI Physical Function is supported, disabling the first port causes the second port to disappear as well.
- The NIC does not notify the driver of a link-down incident when a cable is unplugged from a NIC port with 56GbE port link.
- 56GbE link is not raised when using 100GbE optic cables.
- When working with MLNX_OFED v3.3-1.0.0.0, server reboot could get stuck due to a kernel panic in mlx-4_en_get_drvinfo() that is called from asynchronous event handler.
- 832298:When running ibdump, loopback traffic is mirroring into the kernel driver.
- AHS reports wrong MTU size
- RM#846523: MAC address that are set from the OS using ifconfig are not reflected in the OCBB buffer.

Known Issues for FW version 14.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
- Health counter increases every 50ms instead of 10ms.
- mlxconfig tool presents all possible expansion ROM images instead of presenting only the existing images.
- An ethernet multicas loopback packet is not counted (even if it is not local loopback packets)when running the nic_receive_steering_discard command.
- When a dual-port VHCA sends RoCE packets on its non-native port, and the packet arrives to its affiliated vport FDB, a mismatch might happen on the rules that match the packet source vport.

Known Issues for FW version 12.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
- On rare occasions, retransmissions/packet loss under signature can cause error reporting and terminate the connection.
- Health counter increases every 50ms instead of 10ms.

- mlxconfig tool presents all possible expansion ROM images, instead of presenting only the existing images.
- An Ethernet multicast loopback packet is not counted (even if it is not a local loopback packet) when running the nic_receive_steering_discard command.
- When a dual-port VHCA sends a RoCE packet on its non-native port. and the packet arrives to its affiliated vport FDB, a mismatch might happen on the rules that match the packet source vport.
- During DC CNAK stress tests, DC CNAK timeout (CNAK drops) might occur.

Known Issues for FW version 16.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
- Health counter increases every 50ms instead of 10ms.

Prerequisites

HPE Synergy 6410C 25/50Gb Ethernet Adapter (868779-B21) must first be upgraded to prerequisite firmware version 12.21.2808 before updating to 12.22.0148 or 12.22.0194.
12.22.0194 is the first secure firmware for HPE Synergy 6410C 25/50Gb Ethernet Adapter (868779-B21). Once this device is upgraded to firmware 12.22.0194, downgrade is not allowed.

Fixes

Fixes submitted in version 2.42.5000 :

- The PortRcvPkts counter was prevented from being cleared after resetting it..
- System Time Out on the configuration cycle of the VFs when more than 10 Virtual Functions performed FLR and the completion Time Out value was configured to a range of less than 16 msec.
- The server hung and resulted in NMI (Non-maskable interrupt) when run-ning "mlxfwtop –d mt4103_pci_cr0" while restarting the driver in parallel (from a differ-ent thread). In this case, the downstream bridge over the device reported completion timeout error.
- In flow_steering, BMC could not receive a ping over IPV6 after running bmc_reboot.
- While closing the HCA (Host Channel Adapters), RX packet caused bad access to resources that did not exist, and consequently caused the QPCGW or the irisc to get stuck.
- The master SMLID and the LID was either 0 or 0xFFFF when the port was neither active nor armed.
- ibdump could not capture all MADs packets.
- Link could not go up after reboot.
- A rare issue caused the PCIe configuration cycle that arrived during the time of sw_reset to generate 2 completions.
- NC-SI (Network Controller Sideband Interface) did not work when adding the disable_stat-ic_steering_ini field in the ini file, due to memory allocation issue for this field in the scratchpad.

Fixes submitted in version 14.22.1414 :

- A temperature normalization function calculation issue. Now the cable gain that is not pure integer is taken into account was fixed.
- An issue related to the parser of object 0x8 in ASN that caused different structure in response was fixed.
- Added the option to avoid unintentionally powering off the backplane port cage upon reboot when in standby mode.
- An issue that caused the driver to return a wrong logical OR of the 2 physical ports, when querying the vport state when the LAG was enabled wre fixed.
- Increased the Full Wire Speed (FWS) threshold value to improve EDR link results.
- An issue that resulted in "Destroy LAG" command failure if a VFs received an FLR while its affinity QPs were open.
- When RoCE Dual Port mode is enabled, tcpdump is not functional on the 2nd port.

Enhancements

Firmware for the following devices are updated to 2.42.5000:

779799-B21 (HP Ethernet 10G 2-port 546FLR-SFP+ Adapter)
779793-B21 (HP Ethernet 10G 2-port 546SFP+ Adapter)

New features and changes in version 2.42.5000:

Added support for the following features:
TLV: CX3_GLOBAL_CONF to enable/disable timestamp on incoming packets through mlxconfig configuration.
User MAC configuration.
Automatically collecting mstdump before driver reset.
to detect DEAD_IRISC (plastic) from TPT (iron) and raise an assert.
Enhanced the debug ability for command timeout cases.
Added a new field to "set port" command which notifies the firmware what is the user_mtu size.

Firmware for the following devices are updated to 14.22.1414 :

817749-B21 (HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter)
817753-B21 (HPE Ethernet 25Gb 2-port 640SFP28 Adapter)

New features and changes in version 14.22.1414:

Transition from 4MB to 7M Firmware Image Banks.
Software Reset Flow: Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
Steering Discard Packet Counters: The following counters were added to count the discard packets (per vport)
nic_receive_steering_discard
receive_discard_vport_down
transmit_discard_vport_down

- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow
  - in dual port devices to 20 VFs
  - in single port devices to 58 VFs
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Firmware for the following device is updated to 12.22.1414 :

868779-B21 (HPE Synergy 6410C 25/50Gb Ethernet Adapter)

New features and changes in version 12.22.1414:

- Transition from 4MB to 7M Firmware Image Banks.
- **Software Reset Flow:** Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
- **Steering Discard Packet Counters:** The following counters were added to count the discard packets (per vport)
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow
  - in dual port devices to 20 VFs
  - in single port devices to 58 VFs
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Firmware for the following device is updated to 16.22.1414 :

874253-B21 (HPE Ethernet 100Gb 1-port 842QSFP28 Adapter)

New features and changes in version 16.22.1414:

- Transition from 4MB to 7M Firmware Image Banks.
- **Software Reset Flow:** Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
- **Steering Discard Packet Counters:** The following counters were added to count the discard packets (per vport)
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- Added support for Push/Pop VLAN, new FLOW TABLE ENTRY actions. These new actions are used by the driver to implement Q-in-Q functionality.
- Packet Pacing in ConnectX-5 adapter cards.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Supported Devices and Features

HPE Part Number	InfiniBand Card Type	PSID
779793-B21	HP Ethernet 10Gb 2-port 546SFP+ Adapter	HP_1200111023
779799-B21	HP Ethernet 10Gb 2-port 546FLR-SFP+ Adapter	HP_2240110004
817749-B21	HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter	HP_2690110034
817753-B21	HPE Ethernet 25Gb 2-port 640SFP28 Adapter	HP_2420110034
868779-B21	HPE Synergy 6410C 25/50Gb Ethernet Adapter	HPE0000000006

874253-B21	HPE Ethernet 100Gb 1-port 842QSFP28 Adapter	HPE0000000014

Online Firmware Upgrade Utility (ESXi 6.0) for HPE Mellanox VPI (Ethernet and Infiniband mode) ConnectX4 and ConnectX5 devices on VMware ESXi 6.0
Version: 1.0.4 **(Recommended)**
Filename: CP034538.compsig; CP034538.zip

Important Note!

Known Issues in firmware version 12.22.4030 and 16.22.4030:

- The maximum "read" size of MTRC_STDB is limited by 272 Bytes.
- Using vl_arb_high or vl_arb_low simultaneously might cause unexpected behavior in QoS functionality.

Prerequisites

Due to significant firmware changes, the devices mentioned in the table below must be upgraded to the prerequisite version first, then programmed to version 16.22.0194 and onwards.
16.22.0194 is the first secure firmware for HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter (879482-B21). Once this device is upgraded to firmware 16.22.0194, downgrade is not allowed.

InfiniBand Card Type	Prerequisite firmware version
HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter (872726-B21)	16.21.2808
HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter (879482-B21)	16.21.2800

Fixes

Fixes in firmware version 12.22.4030 and 16.22.4030:

- In rare cases, where the width of the receiver's electrical eye is narrow, the link might raise with BER lower than 10^-12.
- LRO timeout configuration is now taken from the TLV configuration instead of the static defined values.
- Added a filter to ignore module temperature reads below -40C and above 125C.
- Closed the vport as part of the fast teardown flow, to prevent Ack to be sent without been scatter to memory.
- A rare scenario where the PERST# de-assertion arrived at a specific critical time period was handled.
- Temperature normalization function calculation issue. Now the cable gain that is not pure integer is taken into account.
- The parser of object 0x8 in ASN that caused different structure in response.
- An issue that caused MSIX interrupt lost while the HCA performed an FLR was handled.
- An issue that caused a race condition between the firmware boot process and the MSIX access from the PCIe, which resulted in lost writes into the MSIX vector was fixed.

Enhancements

Firmware for the following devices are updated to 12.22.4030:

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter)

New features and changes in version 12.22.4030:

- **AS Notify:** AS Notify enables IBM's Power CPU architecture to boost performance by allowing the hardware to issue light weight "interrupts" to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.
- **Port Enable:** When set, the device supports emulating link down for all the associated functions using "ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters".
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.

Firmware for the following devices are updated to 16.22.4030:

879482-B21 (HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter)
872726-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter)

New features and changes in version 16.22.4030:

- **AS Notify:** AS Notify enables IBM's Power CPU architecture to boost performance by allowing the hardware to issue light weight "interrupts" to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.

- **Port Enable:** When set, the device supports emulating link down for all the associated functions using "ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters".
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.
- Added support for striding RQ in InfiniBand.
- **QoS "Rate Limit":** Added support to limit the transmission rate of individual InfiniBand port Service Levels. This capability is configurable through a new vendor-specific MAD (QosConfigSL).

Supported Devices and Features

HPE Part Number	Device Name	PSID
825110-B21	HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter	HP_2180110032
825111-B21	HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter	HP_2190110032
872726-B21	HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter	HPE0000000009
879482-B21	HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter	HPE0000000022

Online Firmware Upgrade Utility (ESXi 6.0) for HPE Mellanox VPI (Ethernet and Infiniband mode) devices on VMware ESXi 6.0
Version: 1.0.6 **(Recommended)**
Filename: CP033386.compsig; CP033386.zip

Important Note!

Known Issues in firmware 2.40.5030, 2.40.5072, 2.42.5000, 2.42.5004:

- Downgrading from v2.30.8000 or later to an earlier version than 2.30.8000 requires server reboot.
  Workaround: Reboot the server.
- On ConnectX-3 Ethernet adapter cards, there is a mismatch between the GUID value returned by firmware management cards tools and that returned by fabric/driver utilities that read the GUID via device firmware (e.g., using ibstat). Mlxburn/flint return 0xffff as GUID while the utilities return a value derived from the MAC address. For all driver/firmware/software purposes, the latter value should be used.
  Workaround: Use the GUID value returned by the fabric/driver utilities (not 0xffffff).
- SBR should be asserted for a minimum of 50 milliseconds for the ConnectX®-3 adapters.
- On Pilot1 SL230, PCIe link occasionally does not come up at Gen3 speed.
- RH6.3 Inbox driver causes kernel panic when SR-IOV is enabled on VPI cards due to driver compatibility issue.
- In advanced steering mode, side band management connectivity may be lost when having more than 8 QP per mcg.
- When SR-IOV is disabled in the system BIOS, a PCI issue is noticed in Ubuntu v12.04.3 with Linux kernel v3.8 which affects NICs of several manufacturers including Mellanox's, preventing them from operating.
  Workaround: Enable SR-IOV in the BIOS.
- MFT tools might leave the flash semaphore locked if the tool operation is forced stopped. The locked semaphore prevents the firmware from accessing the flash and causes firmware hang..
  Workaround: Clear the semaphore using MFT command: flint -clear_semaphore
- Cable Info MAD reports a wrong cable info when using the MC2210411-SR4 module.
- Gen2 failure at temperature sweep up to 10C/min (for MT27518A1-FDIR-BV only).
- PCIe Gen2 link unstable at temperature sweep of 10C/min for MT27518A1-FDIR-BV.
- Bloom filter is currently not supported.
- When downgrading from firmware v2.11.0000 and using MFT 3.0.0-3, Release the following message is displayed due to the mlxconfig tool:
  DMFS steering mode with IB in Linux You are trying to override configurable FW by non-configurable FW. If you continue, old FW configurations will be cleared, do youwant to continue ? (y/n) [n] : y
  You are trying to restore default configuration, do you want to continue ? (y/n) [n] :y
- DMFS should not be enabled when working with InfiniBand on MLNX_OFED-2.0.3.
  Workaround: Upgrade to MLNX_OFED-2.1-x.x.x. or later.
- VPD read-only fields are writable.
  Workaround: Do not write to read- only fields if you wish to preserve them.
- When working in VPI mode with port1 FDR and port2 40G, error counters misbehave and increase rapidly.
- Setting the device to 128Byte CQ/EQ stride will cause misbehavior of sideband management resulting in communication loss.
- CQ and EQ cannot be configured to different stride sizes.
- ConnectX-3 Pro VF device ID is presented the same as.ConnectX-3 VF device ID due to driver limitations.
  Workaround: Use the physical function device ID to identify the device.
- Changing port protocol from ETH to IB on port with NCSI/IPMI enabled while the port is connected to ETH switch is not supported.
  Workaround:
  - Unplug the cable from the switch
  - Restart driver
  - Change the protocol via the appropriate tools.
- RDP over IPv6 is currently not functional.
  Workaround: Set the default RoCE mode in the software to RoCE v2 (also when not using RoCE).
- Sniffer QP cannot be removed from the regular rule after adding the QP with insertion scheme equals to "push to that rule".
- Since only a single Boot Entry Vector (BEV) per PCI Physical Function is supported, disabling the first port causes the second port to disappear as well.
- The NIC does not notify the driver of a link-down incident when a cable is unplugged from a NIC port with 56GbE port link.
- 56GbE link is not raised when using 100GbE optic cables.
- When working with MLNX_OFED v3.3-1.0.0.0, server reboot could get stuck due to a kernel panic in mlx4_en_get_drvinfo() that is

called from asynchronous event handler.
- When running ibdump, loopback traffic is mirroring into the kernel driver.

Known Issues in firmware version 2.42.5000, 2.42.5004:

- Enabling/disabling cq_timestamp using mlxconfig is not supported.
- In a card with 2 separate LEDs scheme (a Phy LED and a logic LED) only the Phy LED will lit. Meaning, the orange LED will not be active while the ETH link is in an idle mode.
- In SR-IOV (Single Root I/O Virtualization) setup, using mlxconfig when the PF (Physical Function) is passed through to a VM (Virtual Machine) requires a reboot of the Hypervisor.
- Adapter card MCX349A-XCCN may experience longer linkup times of a few seconds with specific switches.
- Adapter card MCX349A-XCCN does not respond to ethtool "identify" command (ethtool -p/--identify).
- MAC address that are set from the OS using ifconfig are not reflected in the OCBB buffer.

Known Issues in firmware version 2.40.5072:

- Ambient sensor does not report via Platform Level Data Model (PLDM) in GEN10 connectX3.

Known Issues in firmware version 2.42.5000:

- MTUSB communication via I2C header on primary I2C bus is supported only in live-fish mode.

Known Issues in firmware version 2.42.5004:

- Cisco bi-directional transceiver is not supported in HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter.

Fixes

Fixes in version 2.40.5030 and 2.40.5072:

- Race between the firmware and the hardware during driver start which blocked outbound completions.
- The firmware did not send link_down event to the driver when running the close_port command.

Fixes in version 2.42.5000:

- PortRcvPkts counter was prevented from being cleared after resetting it.
- The system Timed Out on the configuration cycle of the Virtual Functions (VFs) when more than 10 Virtual Functions performed FLR and the completion Time Out value was configured to a range of less than 16 msec.
- The server hangs and results in NMI when running "mlxfwtop –d mt4103_pci_cr0" while restarting the driver in parallel (from a different thread). In this case, the downstream bridge over the device reported completion timeout error.
- In flow_steering, BMC could not receive a ping over IPV6 after running bmc_reboot.
- While closing the HCA, the RX packet caused bad access to resources that did not exist, and consequently caused the QPCGW or the irisc to get stuck.
- The master SMLID and the LID was either 0 or 0xFFFF when the port was neither active nor armed.
- ibdump could not capture all MADs packets.
- link did not go up after reboot.
- Fixed a rare issue that cause the PCIe configuration cycle that arrived during the time of sw_reset to generate 2 completions.
- Network Controller Sideband Interface (NC-SI) did not work when adding the disable_static_steering_ini field in the ini file, due to memory allocation issue for this field in the scratchpad.

Fixes in version 2.42.5004:

- In UEFI (Unified Extensible Firmware Interface) HII (Human Interface Infrastructure) menu, when using HPE Gen10 devices, both ports appear as port 1.
- In UEFI (Unified Extensible Firmware Interface) boot menu, when using HPE Gen10 devices, the device name appears with an unneeded port number.

Enhancements

Firmware for the following devices are updated to 2.40.5030:
764286-B21
778509-B21

Firmware for the following devices are updated to 2.40.5072:
764285-B21

Firmware for the following devices are updated to 2.42.5004:
764283-B21
764284-B21

Firmware for the following devices are updated to 2.42.5000:
764282-B21

New features in firmware version 2.40.5030:

- Added support for the following features.
  - Temperature thresholds high/low default for MAD sensing and NCSI/IPMI OEM commands.
  - A new field is added to "set port" command which notifies the firmware what is the user_mtu size.
  - A protection mechanism which ensures the firmware drops packets which are received in internal Queue Pairs (QPs) and disables the WQE producer fetching.

New features in firmware version 2.40.5072:

- Platform Level Data Model (PLDM) support.

New features in firmware version 2.42.5000:

- Added support for the following features.
  - new TLV: CX3_GLOBAL_CONF to enable/disable timestamp on incoming packets through mlxconfig configuration.
  - User MAC configuration.
  - Automatically collecting mstdump before driver reset.
  - A mechanism to detect DEAD_IRISC (plastic) from TPT (iron) and raise an assert.
  - A new field is added to "set port" command which notifies the firmware what is the user_mtu size.
- Improved the debug ability for command timeout cases

Supported Devices and Features

Supported Devices:

HP Part Number	Device Name	PSID
764282-B21	HP InfiniBand QDR/Ethernet 10Gb 2-port 544+M Adapter	HP_1350110023
764283-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M Adapter	HP_1360110017
764284-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter	HP_1370110017
764285-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP Adapter	HP_1380110017
764286-B21	HP InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP Adapter	HP_1390110023

Online Firmware Upgrade Utility (ESXi 6.5) for HPE Mellanox Ethernet only adapters
Version: 1.0.3 **(Recommended)**
Filename: CP034530.compsig; CP034530.zip

Important Note!

Known Issues for FW version 2.42.5000 :

- Enabling/disabling cq_timestamp using mlxconfig is not supported.
- In a card with 2 separate LEDs scheme (a Phy LED and a logic LED) only the Phy LED will lit. Meaning, the orange LES will not be active while the ETH link is in an idle mode.
- In SR-IOV setup, using mlxconfig when the PF is passed through to a VM requires a reboot of the Hypervisor.
- Downgrade to previous GA requires server reboot.Downgrading from v2.30.8000 or later to an earlier version than 2.30.8000 requires server reboot. Reboot the server.
- On ConnectX-3 Ethernet adapter cards, there is a mismatch between the GUID value returned by firmware management tools and that returned by fabric/driver utilities that read the GUID via device firmware (e.g., using ibstat). Mlxburn/flint return 0xffff as GUID while the utilities return a value derived from the MAC address. For all driver/firmware/software purposes, the lattervalue should be used.
- SBR should be asserted for a minimum of 50 milliseconds for the ConnectX®-3 adapters
- On Pilot1 SL230, PCIe link occasionally does not come up at Gen3 speed
- RH6.3 Inbox driver causes kernel panic when SR-IOV is enabled on VPI cards due to driver compatibility issue.
- In advanced steering mode, side band management connectivity may be lost when having more than 8 QP per mcg.
- When SR-IOV is disabled in the system BIOS, a PCI issue is noticed in Ubuntu v12.04.3 with Linux kernel v3.8 which affects NICs of several manufacturers including Mellanox's, preventing them from operating.
- MFT tools might leave the flash semaphore locked if the tool operation is forced stopped. The locked semaphore prevents the firmware from accessing the flash and causes firmware hang.
- Cable Info MAD reports a wrong cable info when usingthe MC2210411-SR4 module
- Gen2 failure at temperature sweep up to 10C/min (for MT27518A1-FDIR-BV only).

- PCIe Gen2 link unstable at temperature sweep of 10C/min for MT27518A1-FDIR-BV
- Bloom filter is currently not supported.
- Firmware downgrade message When downgrading from firmware v2.11.0000 and using MFT 3.0.0-3
- RM#DMFS should not be enabled when working with InfiniBand on MLNX_OFED-2.0.3
- RM#VPD read-only fields are writable.
- Increasing SymbolErrorCounter When working in VPI mode with port1 FDR and port2 40G, error counters misbehave and increase rapidly
- Setting the device to 128Byte CQ/EQ stride will cause misbehavior of sideband management resulting in communication loss.
- CQ and EQ cannot be configured to different stride sizes.
- ConnectX-3 Pro VF device ID is presented the same as ConnectX-3 VF device ID due to driver limitations.
- RSOD while running PXE (legacy) on G9 servers. This occurs only when PXE boot fails and BIOS boots from HDD. Currently it is pending BIOS fix.
- Changing port protocol from ETH to IB on port with NCSI/IPMI enabled while the port is connected to ETH switch is not supported.
- RDP over IPv6 is currently not functional.
- Sniffer QP cannot be removed from the regular rule after adding the QP with insertion scheme equals to "push to that rule"
- Since only a single Boot Entry Vector (BEV) per PCI Physical Function is supported, disabling the first port causes the second port to disappear as well.
- The NIC does not notify the driver of a link-down incident when a cable is unplugged from a NIC port with 56GbE port link.
- 56GbE link is not raised when using 100GbE optic cables.
- When working with MLNX_OFED v3.3-1.0.0.0, server reboot could get stuck due to a kernel panic in mlx-4_en_get_drvinfo() that is called from asynchronous event handler.
- 832298:When running ibdump, loopback traffic is mirroring into the kernel driver.
- AHS reports wrong MTU size
- RM#846523: MAC address that are set from the OS using ifconfig are not reflected in the OCBB buffer.

Known Issues for FW version 14.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
- Health counter increases every 50ms instead of 10ms.
- mlxconfig tool presents all possible expansion ROM images instead of presenting only the existing images.
- An ethernet multicas loopback packet is not counted (even if it is not local loopback packets)when running the nic_receive_steering_discard command.
- When a dual-port VHCA sends RoCE packets on its non-native port, and the packet arrives to its affiliated vport FDB, a mismatch might happen on the rules that match the packet source vport.

Known Issues for FW version 12.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
- On rare occasions, retransmissions/packet loss under signature can cause error reporting and terminate the connection.
- Health counter increases every 50ms instead of 10ms.
- mlxconfig tool presents all possible expansion ROM images, instead of presenting only the existing images.
- An Ethernet multicast loopback packet is not counted (even if it is not a local loopback packet) when running the nic_receive_steering_discard command.
- When a dual-port VHCA sends a RoCE packet on its non-native port. and the packet arrives to its affiliated vport FDB, a mismatch might happen on the rules that match the packet source vport.
- During DC CNAK stress tests, DC CNAK timeout (CNAK drops) might occur.

Known Issues for FW version 16.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
- Health counter increases every 50ms instead of 10ms.

Prerequisites

HPE Synergy 6410C 25/50Gb Ethernet Adapter (868779-B21) must first be upgraded to prerequisite firmware version 12.21.2808 before updating to 12.22.0148 or 12.22.0194.
12.22.0194 is the first secure firmware for HPE Synergy 6410C 25/50Gb Ethernet Adapter (868779-B21). Once this device is upgraded to firmware 12.22.0194, downgrade is not allowed.

Fixes

Fixes submitted in version 2.42.5000 :

- The PortRcvPkts counter was prevented from being cleared after resetting it..
- System Time Out on the configuration cycle of the VFs when more than 10 Virtual Functions performed FLR and the completion Time
- Out value was configured to a range of less than 16 msec.
- The server hung and resulted in NMI (Non-maskable interrupt) when run-ning "mlxfwtop –d mt4103_pci_cr0" while restarting the
- driver in parallel (from a differ-ent thread). In this case, the downstream bridge over the device reported completion timeout error.
- In flow_steering, BMC could not receive a ping over IPV6 after running bmc_reboot.
- While closing the HCA (Host Channel Adapters), RX packet caused bad access to resources that did not exist, and consequently caused the QPCGW or the irisc to get stuck.
- The master SMLID and the LID was either 0 or 0xFFFF when the port was neither active nor armed.
- ibdump could not capture all MADs packets.
- Link could not go up after reboot.
- A rare issue caused the PCIe configuration cycle that arrived during the time of sw_reset to generate 2 completions.
- NC-SI (Network Controller Sideband Interface) did not work when adding the disable_stat-ic_steering_ini field in the ini file, due to memory allocation issue for this field in the scratchpad.

Fixes submitted in version 14.22.1414 :

- A temperature normalization function calculation issue. Now the cable gain that is not pure integer is taken into account was fixed.
- An issue related to the parser of object 0x8 in ASN that caused different structure in response was fixed.
- Added the option to avoid unintentionally powering off the backplane port cage upon reboot when in standby mode.
- An issue that caused the driver to return a wrong logical OR of the 2 physical ports, when querying the vport state when the LAG was enabled wre fixed.
- Increased the Full Wire Speed (FWS) threshold value to improve EDR link results.
- An issue that resulted in "Destroy LAG" command failure if a VFs received an FLR while its affinity QPs were open.
- When RoCE Dual Port mode is enabled, tcpdump is not functional on the 2nd port.

Enhancements

Firmware for the following devices are updated to 2.42.5000:

779799-B21 (HP Ethernet 10G 2-port 546FLR-SFP+ Adapter)
779793-B21 (HP Ethernet 10G 2-port 546SFP+ Adapter)

New features and changes in version 2.42.5000:

- Added support for the following features:
  - TLV: CX3_GLOBAL_CONF to enable/disable timestamp on incoming packets through mlxconfig configuration.
  - User MAC configuration.
  - Automatically collecting mstdump before driver reset.
  - to detect DEAD_IRISC (plastic) from TPT (iron) and raise an assert.
- Enhanced the debug ability for command timeout cases.
- Added a new field to "set port" command which notifies the firmware what is the user_mtu size.

Firmware for the following devices are updated to 14.22.1414 :

817749-B21 (HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter)
817753-B21 (HPE Ethernet 25Gb 2-port 640SFP28 Adapter)

New features and changes in version 14.22.1414:

- Transition from 4MB to 7M Firmware Image Banks.
- **Software Reset Flow:** Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
- **Steering Discard Packet Counters:** The following counters were added to count the discard packets (per vport)
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow
  - in dual port devices to 20 VFs
  - in single port devices to 58 VFs
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Firmware for the following device is updated to 12.22.1414 :

868779-B21 (HPE Synergy 6410C 25/50Gb Ethernet Adapter)

New features and changes in version 12.22.1414:

- Transition from 4MB to 7M Firmware Image Banks.
- **Software Reset Flow:** Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
- **Steering Discard Packet Counters:** The following counters were added to count the discard packets (per vport)
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow
  - in dual port devices to 20 VFs
  - in single port devices to 58 VFs
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Firmware for the following device is updated to 16.22.1414 :

874253-B21 (HPE Ethernet 100Gb 1-port 842QSFP28 Adapter)

New features and changes in version 16.22.1414:

- Transition from 4MB to 7M Firmware Image Banks.
- **Software Reset Flow:** Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
- **Steering Discard Packet Counters:** The following counters were added to count the discard packets (per vport)
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- Added support for Push/Pop VLAN, new FLOW TABLE ENTRY actions. These new actions are used by the driver to implement Q-in-Q functionality.
- Packet Pacing in ConnectX-5 adapter cards.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Supported Devices and Features

HPE Part Number	InfiniBand Card Type	PSID
779793-B21	HP Ethernet 10Gb 2-port 546SFP+ Adapter	HP_1200111023
779799-B21	HP Ethernet 10Gb 2-port 546FLR-SFP+ Adapter	HP_2240110004
817749-B21	HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter	HP_2690110034
817753-B21	HPE Ethernet 25Gb 2-port 640SFP28 Adapter	HP_2420110034
868779-B21	HPE Synergy 6410C 25/50Gb Ethernet Adapter	HPE0000000006
874253-B21	HPE Ethernet 100Gb 1-port 842QSFP28 Adapter	HPE0000000014

Online Firmware Upgrade Utility (ESXi 6.5) for HPE Mellanox VPI (Ethernet and Infiniband mode) ConnectX4 and ConnectX5 devices on VMware ESXi 6.5
Version: 1.0.3 **(Recommended)**
Filename: CP034539.compsig; CP034539.zip

Important Note!

Known Issues in firmware version 12.22.4030 and 16.22.4030:

- The maximum "read" size of MTRC_STDB is limited by 272 Bytes.
- Using vl_arb_high or vl_arb_low simultaneously might cause unexpected behavior in QoS functionality.

Prerequisites

Due to significant firmware changes, the devices mentioned in the table below must be upgraded to the prerequisite version first, then programmed to version 16.22.0194 and onwards.
16.22.0194 is the first secure firmware for HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter (879482-B21). Once this device is upgraded to firmware 16.22.0194, downgrade is not allowed.

InfiniBand Card Type	Prerequisite firmware version
HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter (872726-B21)	16.21.2808
HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter (879482-B21)	16.21.2800

Fixes

Fixes in firmware version 12.22.4030 and 16.22.4030:

- In rare cases, where the width of the receiver's electrical eye is narrow, the link might raise with BER lower than 10^-12.
- LRO timeout configuration is now taken from the TLV configuration instead of the static defined values.
- Added a filter to ignore module temperature reads below -40C and above 125C.
- Closed the vport as part of the fast teardown flow, to prevent Ack to be sent without been scatter to memory.
- A rare scenario where the PERST# de-assertion arrived at a specific critical time period was handled.
- Temperature normalization function calculation issue. Now the cable gain that is not pure integer is taken into account.
- The parser of object 0x8 in ASN that caused different structure in response.
- An issue that caused MSIX interrupt lost while the HCA performed an FLR was handled.
- An issue that caused a race condition between the firmware boot process and the MSIX access from the PCIe, which resulted in lost writes into the MSIX vector was fixed.

Enhancements

Firmware for the following devices are updated to 12.22.4030:

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter)

New features and changes in version 12.22.4030:

- **AS Notify:** AS Notify enables IBM's Power CPU architecture to boost performance by allowing the hardware to issue light weight "interrupts" to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.
- **Port Enable:** When set, the device supports emulating link down for all the associated functions using "ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters".
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.

Firmware for the following devices are updated to 16.22.4030:

879482-B21 (HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter)
872726-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter)

New features and changes in version 16.22.4030:

- **AS Notify:** AS Notify enables IBM's Power CPU architecture to boost performance by allowing the hardware to issue light weight "interrupts" to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.
- **Port Enable:** When set, the device supports emulating link down for all the associated functions using "ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters".
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.
- Added support for striding RQ in InfiniBand.
- **QoS "Rate Limit":** Added support to limit the transmission rate of individual InfiniBand port Service Levels. This capability is configurable through a new vendor-specific MAD (QosConfigSL).

Supported Devices and Features

HPE Part Number	Device Name	PSID
825110-B21	HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter	HP_2180110032
825111-B21	HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter	HP_2190110032
872726-B21	HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter	HPE0000000009
879482-B21	HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter	HPE0000000022

Online Firmware Upgrade Utility (ESXi 6.5) for HPE Mellanox VPI (Ethernet and Infiniband mode) devices on VMware ESXi 6.5
Version: 1.0.1 **(Recommended)**
Filename: CP033387.compsig; CP033387.zip

Important Note!

Known Issues in firmware 2.40.5030, 2.40.5072, 2.42.5000, 2.42.5004:

- Downgrading from v2.30.8000 or later to an earlier version than 2.30.8000 requires server reboot.
  Workaround: Reboot the server.
- On ConnectX-3 Ethernet adapter cards, there is a mismatch between the GUID value returned by firmware management cards tools and that returned by fabric/driver utilities that read the GUID via device firmware (e.g., using ibstat). Mlxburn/flint return 0xffff as GUID while the utilities return a value derived from the MAC address. For all driver/firmware/software purposes, the latter value should be used.
  Workaround: Use the GUID value returned by the fabric/driver utilities (not 0xffffff).
- SBR should be asserted for a minimum of 50 milliseconds for the ConnectX®-3 adapters.
- On Pilot1 SL230, PCIe link occasionally does not come up at Gen3 speed.
- RH6.3 Inbox driver causes kernel panic when SR-IOV is enabled on VPI cards due to driver compatibility issue.
- In advanced steering mode, side band management connectivity may be lost when having more than 8 QP per mcg.
- When SR-IOV is disabled in the system BIOS, a PCI issue is noticed in Ubuntu v12.04.3 with Linux kernel v3.8 which affects NICs of several manufacturers including Mellanox's, preventing them from operating.
  Workaround: Enable SR-IOV in the BIOS.

MFT tools might leave the flash semaphore locked if the tool operation is forced stopped. The locked semaphore prevents the firmware from accessing the flash and causes firmware hang..
Workaround: Clear the semaphore using MFT command: flint -clear_semaphore
- Cable Info MAD reports a wrong cable info when using the MC2210411-SR4 module.
- Gen2 failure at temperature sweep up to 10C/min (for MT27518A1-FDIR-BV only).
- PCIe Gen2 link unstable at temperature sweep of 10C/min for MT27518A1-FDIR-BV.
- Bloom filter is currently not supported.
- When downgrading from firmware v2.11.0000 and using MFT 3.0.0-3, Release the following message is displayed due to the mlxconfig tool:
  DMFS steering mode with IB in Linux You are trying to override configurable FW by non-configurable FW. If you continue, old FW configurations will be cleared, do youwant to continue ? (y/n) [n] : y
  You are trying to restore default configuration, do you want to continue ? (y/n) [n] :y
- DMFS should not be enabled when working with InfiniBand on MLNX_OFED-2.0.3.
  Workaround: Upgrade to MLNX_OFED-2.1-x.x.x. or later.
- VPD read-only fields are writable.
  Workaround: Do not write to read- only fields if you wish to preserve them.
- When working in VPI mode with port1 FDR and port2 40G, error counters misbehave and increase rapidly.
- Setting the device to 128Byte CQ/EQ stride will cause misbehavior of sideband management resulting in communication loss.
- CQ and EQ cannot be configured to different stride sizes.
- ConnectX-3 Pro VF device ID is presented the same as.ConnectX-3 VF device ID due to driver limitations.
  Workaround: Use the physical function device ID to identify the device.
- Changing port protocol from ETH to IB on port with NCSI/IPMI enabled while the port is connected to ETH switch is not supported.
  Workaround:
  - Unplug the cable from the switch
  - Restart driver
  - Change the protocol via the appropriate tools.
- RDP over IPv6 is currently not functional.
  Workaround: Set the default RoCE mode in the software to RoCE v2 (also when not using RoCE).
- Sniffer QP cannot be removed from the regular rule after adding the QP with insertion scheme equals to "push to that rule".
- Since only a single Boot Entry Vector (BEV) per PCI Physical Function is supported, disabling the first port causes the second port to disappear as well.
- The NIC does not notify the driver of a link-down incident when a cable is unplugged from a NIC port with 56GbE port link.
- 56GbE link is not raised when using 100GbE optic cables.
- When working with MLNX_OFED v3.3-1.0.0.0, server reboot could get stuck due to a kernel panic in mlx4_en_get_drvinfo() that is called from asynchronous event handler.
- When running ibdump, loopback traffic is mirroring into the kernel driver.

Known Issues in firmware version 2.42.5000, 2.42.5004:

- Enabling/disabling cq_timestamp using mlxconfig is not supported.
- In a card with 2 separate LEDs scheme (a Phy LED and a logic LED) only the Phy LED will lit. Meaning, the orange LED will not be active while the ETH link is in an idle mode.
- In SR-IOV (Single Root I/O Virtualization) setup, using mlxconfig when the PF (Physical Function) is passed through to a VM (Virtual Machine) requires a reboot of the Hypervisor.
- Adapter card MCX349A-XCCN may experience longer linkup times of a few seconds with specific switches.
- Adapter card MCX349A-XCCN does not respond to ethtool "identify" command (ethtool -p/--identify).
- MAC address that are set from the OS using ifconfig are not reflected in the OCBB buffer.

Known Issues in firmware version 2.40.5072:

- Ambient sensor does not report via Platform Level Data Model (PLDM) in GEN10 connectX3.

Known Issues in firmware version 2.42.5000:

- MTUSB communication via I2C header on primary I2C bus is supported only in live-fish mode.

Known Issues in firmware version 2.42.5004:

- Cisco bi-directional transceiver is not supported in HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter.

Fixes

Fixes in version 2.40.5030 and 2.40.5072:

- Race between the firmware and the hardware during driver start which blocked outbound completions.
- The firmware did not send link_down event to the driver when running the close_port command.

Fixes in version 2.42.5000:

- PortRcvPkts counter was prevented from being cleared after resetting it.
- The system Timed Out on the configuration cycle of the Virtual Functions (VFs) when more than 10 Virtual Functions performed FLR and the completion Time Out value was configured to a range of less than 16 msec.
- The server hangs and results in NMI when running "mlxfwtop –d mt4103_pci_cr0" while restarting the driver in parallel (from a different thread). In this case, the downstream bridge over the device reported completion timeout error.
- In flow_steering, BMC could not receive a ping over IPV6 after running bmc_reboot.
- While closing the HCA, the RX packet caused bad access to resources that did not exist, and consequently caused the QPCGW or the irisc to get stuck.
- The master SMLID and the LID was either 0 or 0xFFFF when the port was neither active nor armed.
- ibdump could not capture all MADs packets.
- link did not go up after reboot.
- Fixed a rare issue that cause the PCIe configuration cycle that arrived during the time of sw_reset to generate 2 completions.

- Network Controller Sideband Interface (NC-SI) did not work when adding the disable_static_steering_ini field in the ini file, due to memory allocation issue for this field in the scratchpad.

Fixes in version 2.42.5004:

- In UEFI (Unified Extensible Firmware Interface) HII (Human Interface Infrastructure) menu, when using HPE Gen10 devices, both ports appear as port 1.
- In UEFI (Unified Extensible Firmware Interface) boot menu, when using HPE Gen10 devices, the device name appears with an unneeded port number.

Enhancements

Firmware for the following devices are updated to 2.40.5030:
764286-B21
778509-B21

Firmware for the following devices are updated to 2.40.5072:
764285-B21

Firmware for the following devices are updated to 2.42.5004:
764283-B21
764284-B21

Firmware for the following devices are updated to 2.42.5000:
764282-B21

New features in firmware version 2.40.5030:

- Added support for the following features.
  - Temperature thresholds high/low default for MAD sensing and NCSI/IPMI OEM commands.
  - A new field is added to "set port" command which notifies the firmware what is the user_mtu size.
  - A protection mechanism which ensures the firmware drops packets which are received in internal Queue Pairs (QPs) and disables the WQE producer fetching.

New features in firmware version 2.40.5072:

- Platform Level Data Model (PLDM) support.

New features in firmware version 2.42.5000:

- Added support for the following features.
  - new TLV: CX3_GLOBAL_CONF to enable/disable timestamp on incoming packets through mlxconfig configuration.
  - User MAC configuration.
  - Automatically collecting mstdump before driver reset.
  - A mechanism to detect DEAD_IRISC (plastic) from TPT (iron) and raise an assert.
  - A new field is added to "set port" command which notifies the firmware what is the user_mtu size.
- Improved the debug ability for command timeout cases

Supported Devices and Features

Supported Devices:

HP Part Number	Device Name	PSID
764282-B21	HP InfiniBand QDR/Ethernet 10Gb 2-port 544+M Adapter	HP_1350110023
764283-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M Adapter	HP_1360110017
764284-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter	HP_1370110017
764285-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP Adapter	HP_1380110017
764286-B21	HP InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP Adapter	HP_1390110023

Online Firmware Upgrade Utility (Linux x86_64) for HPE Infiniband FDR 2P 545QSFP Adapter (HP Part # 702211-B21), HPE Infiniband FDR 2P 545FLR-QSFP Adapter (HP Part # 702212-B21) and HPE Infiniband FDR 2P 545M Adapter (HP Part #702213-B21)
Version: 1.0.6 **(Recommended)**
Filename: firmware-hca-mellanox-infiniband-only-1.0.6-1.1.x86_64.compsig; firmware-hca-mellanox-infiniband-only-1.0.6-1.1.x86_64.rpm

Important Note!

Known Issues:

- Setting the port to 'sleep' state is not supported.
- Link width x1 might get Replay Timer Timeout, on speed change.
- L1 power state enter requests are ignored by the device.
- **[For customers developing custom low level drivers]**
  The device does not recover if the requested number of pages are not supplied during device initialization.
- On rare occasions, SL to VL modification with functioning QPs results in traffic hangs.
- Vport transmit packets are not blocked if vport policy is Down.
- DC transport is not supported when SR-IOV is enabled.
- ibstat reports the link speed as FDR instead of FDR10.
- When connected to an InfiniScale4 based QDR switch, the link might come up as an SDR speed instead of QDR.
- MTUSB communication via I2C header on primary I2C bus is supported only in live-fish mode.
- mlxconfig tool displays some Ethernet only configuration such as RoCE status.
- PF direct pass-through is not supported (since PF FLR is not supported).
- Some Port Control Register do not return to the default value after the last port owner host restarts the driver.
  Workaround: Reboot or reset the driver.
  reboot / mlxfwreset
- Older MFT versions (4.0.0 and 3.8.0) may indicate that the latest GA firmware is old or that it cannot be compared with the existing firmware.
  A message similar to the below will be displayed upon firmware upgrade stage:
  # flint -d <mst device> -i <image> burn
  Current FW version on flash: 12.1100.6630
  New FW version:
  12.0012.0572
  Note: The new FW version is not newer than the current FW version on flash.
  Do you want to continue ? (y/n) [n] : y
  Workaround: Choose one of the options below to upgrade firmware:
  Upgrade to the latest MFT version (4.1.0)
  Type "y" after the note flint provides
  Run flint with the "-force" flag
- Flashing the firmware requires server reboot.Firmware cannot be flashed twice without server reboot after first flashing
  Workaround: Reboot the server after firmware flashing
- **[For customers developing custom low level drivers]**
  VFs internal FLR is not supported in PF teardown HCA command.
  Workaround: Before unloading the PF driver, PF driver must disable all its active VFs by performing the following:
  1. Run the disable_hca command on all the function_ids
  2. Wait until firmware returns all VFs allocated pages.
- **[For customers developing custom low level drivers]**
  VNodeInfo and VPortGuidInfo virtualization Attributes MADs are not supported.
- **[For customers developing custom low level drivers]**
  The value of log_max_ra_res_qp in set_hca_cap command should be the same in all functions.
- Function (PF/VF) TX port counters are not supported.
- Configuring the SM with VL weight 0 on some VL, and running traffic on it, causes the driver to hang during unload.
- Privileged Vport egress traffic is not blocked when Vport is not active.
- When all SLs are mapped to non-VL0, the firmware might hang.
  Workaround: Fix the SL configuration and power cycle the system.
- In an SR-IOV setup, traffic should contain GRH (GID index), traffic without GRH will be forwarded to vport0 ("Host0").
  OpenSM should be configured as follow (opensm.conf):
  • virt_enable should be 2
  • Enable Qos:
  qos TRUE
- end_padding_mode is required in CREATE_QP and not in INIT_2_RTR command as defined in the PRM.
- Burning in firmware on the same device in parallel from multiple interfaces (e.g. PCIe and MTUSB) is not supported.
- Updating a non-voltile configuration of port type TLV more than 50 times might cause system to hang.
  Workaround: Run mlxconfig reset after every 50 consecutive updates of port type TLV.
- mlxconfig configuration of VF_LOG_BAR_SIZE and PF_LOG_BAR_SIZE are ignored and set to 5 (32MB).
- Performing warm reboot during firmware image burning for VPI/IB devices configured with IB port protocol, might cause the device to disappear from the PCIe.
  Workaround: Cold reboot the device instead

Fixes

The following issues are fixed in firmware version 10.16.1058:

- Fixed an issue which caused system fail when enabled SR-IOV.

- Fixed a rare issue which caused the RX to hang when triggered the SRQ limit event.
- Fixed an issue which occasionally caused the RX traffic to hang in DC when received a PCI error on WQE fetch.
- Fixed an issue which caused the mlxconfig configuration of VF_LOG_BAR_SIZE to be ignored and to be set to 5 (32MB).
- Fixed an EEH error from PCI which caused firmware to hang.
- Fixed an issues which occasionally caused the driver to hang during unload on some VLs when configuring the SM with a VL weight 0 and running traffic on it.
- Fixed a rare case which caused an assert reported to the driver when the DC transport was enabled in the following cases: retransmission occurred and the RX received the same packet twice
- Fixed an issue which caused the HCA to hang when enabled /disabled the VFs vports when the VFs GUIDs configuration were overloaded in the steering table.

The following issues are fixed in firmware version 10.16.1038:

- Fixed RSOD bug.
- Fixed an issue causing single port devices to query and write Physical Port TLVs to Port 2.
- Fixed an issue which caused the device to hang when resetting qkey/pkey violation counter via port_info mad.
- Improved RDMA READ bandwidth under packet lost scenario.
- If the PF driver or the tool (e.g. ethtool) use PAOS DOWN command (e.g. by ifconfig down or ip link set down), loopback traffic is blocked for all functions on this port (PF<->VFs / VF<->VF)
  In Multihost loopback, the traffic will be blocked once the firmware receives the PAOS down command from all PFs. However, the loopback traffic will not be blocked when the port is down due to the physical link (for example: cable plugged out, switch port down).
- Fixed an issue which prevented QP permission for reserve lkey to be passed to the memop machine.
- Fixed a MLX QP SL mismatch handling which occurred when the SL in the WQE was different than the SL in the QP.
- Fixed wrongly implementation of SM SL2VL configuration.
- Fixed a DC re-connect flow which in some cases sent bad completion.
- Fixed a DC performance issue; separated DCRs SQ from the DCI SQs.
- Fixed an issue causing the firmware to hang when running ibdiagnet. The received DiagData MAD included the following values:
  - Clear_all = 1
  - PageNum = 0
  - Port_select = 0

  To prevent the firmware from hanging, a port check was added to Set() as well.
- Fixed an issue which caused hardware fatal error when running ibdump.
- Fixed an FDR10 incorrect speed indication reported due to the usage of a translation function from the hardware speed to the PRM speed twice.
- Fixed a Phy manager PCS event handling when the port's next state was disable.
- Fixed an issue that caused invalid data returned by EyeOpening MAD.
- Reduced the VF ICM footprint for VFs.
- Increased the number of regular memory region from 2^21 to 2^22.
- Fixed improper handling of sequential connect packets.
- On rare occasions, after PXE boot, the port speed came up as SDR instead of a higher speed.
- On very rare occasions, firmware wrongly reported board over-temperature warning.
- destroy-DCT command handling may experience delays while the DCT port is down.
- Fixed an issue causing diagnostic counters VS-MAD page offset to start at a wrong address.
- Fixed stability issue in the event of no-local-DC-resources.
- Fixed improper handling of multiple DCT errors.
- Fixed bad handling of DC RNR state.
- Reduced DCT destroy firmware handling time.
- Fixed link flapping issue which occurred when LLR was active.
- Deprecated code 0x0c0600 was changed to 0x020700 (InfiniBand network adapter).
- Atomic response endianess is always a big endian.
- **[Documentation fix in PRM v2.01, no changes to the firmware code.]**
  Port asynchronous events documentation are different from the PRM. All port events have a type value of 0x9.
  The following subtype values are used for the following events:
  - link down=0x1
  - link up=0x4
  - link initialized=0x5
  - lid change=0x6
  - PKEY change=0x7
  - GUID change=0x8
  - client reregister=0x9
- Alternate Path Migration (APM) triggers only a single affiliated asynchronous error event in the case of a path migration failure.
- Using a min_rnr_nak value of 0x5 will cause failures when creating reliable connection (RC) QPs.
- On rare occasions DC Initiator completions might be lost.
- The following signature rules are not supported (Numbering based on "signature rules table" in PRM):
  - Rule #12: T10 DIF
  - Rule #13: T10 DIF CS
  - Rule #14 T10 DIF CS
- VL arbitration configuration does not ensure minimum bandwidth for VL as configured.
- On very rare occasions, a false firmware “hanged” report is printed in the dmesg.
- CQ buffer resize not supported.
- When connecting to InfiniScale family switches and non-Mellanox InfiniBand switches DDR and QDR speeds may show line errors and in some cases might downgrade to SDR speed.

Enhancements

Firmware for the following devices are updated to 10.16.1038:

702211-B21 (HP Infiniband FDR 2P 545QSFP Adapter)

702212-B21 (HP Infiniband FDR 2P 545FLR-QSFP Adapter)

Firmware for the following devices are updated to 10.16.1058:

702213-B21 (HP Infiniband FDR 2P 545M Adapter)

New features in firmware version 10.16.1038:

- Increased the number of VFs from 32 to 64 per PF.
  Note: When increasing the number of VFs, the following limitations must be taken into consideration:
  • server_total_bar_size >= (num_pfs)*(2log_pf_uar_bar_size + 2log_vf_uar_bar_size*total_vfs)
  • server_total_msix >=(num_pfs)*(num_pf_msix + num_vfs_msix * total_vfs)
- Added v1, v3, v6 tags to VPD read only tag.

Supported Devices and Features

Supported Devices:

HP Part #	Device Name	PSID
702211-B21	HPE Infiniband FDR 2P 545QSFP Adapter	HP_02B0110019
702212-B21	HPE Infiniband FDR 2P 545FLR-QSFP Adapter	HP_02C0110019
702213-B21	HPE Infiniband FDR 2P 545M Adapter	HP_02A0110019

Online Firmware Upgrade Utility (Linux x86_64) for HPE Intel OPA adapters
Version: 1.6.0 (A) **(Recommended)**
Filename: firmware-nic-intel-opa-hfi-1.6.0-2.1.x86_64.compsig; firmware-nic-intel-opa-hfi-1.6.0-2.1.x86_64.rpm

Important Note!

The smart component requires Intel IFS or Basic software v10.6.1.0.2 to be installed as a prerequisite. This software is not part of SPP, but available via HPE.com Support Center and HPE Software Delivery Repository (https://downloads.linux.hpe.com/SDR/index.html)

Offline firmware update is not supported for Intel OPA Smart Component due to this additional software dependency.

Prerequisites

The smart component requires Intel IFS or Basic software v10.6.1.0.2 to be installed as a prerequisite.

Fixes

Fixes in version 1.6.0(A):

1. Update the TMM of all the selected OPA HFI adaptor instead of just the default first adapter
2. Removed duplicate CP.xml and payload.json files.

Supported Devices and Features

HP Part Number	OPA HFI Adapter Type	SSID
829334-B21	HPE 100Gb 1-Port OP101 QSFP28 x8 OPA Adapter	E7
829335-B21	HPE 100Gb 1-Port OP101 QSFP28 x16 OPA Adapter	E8
851226-B21	HPE Apollo 100Gb 1-port Intel Omni-Path Architecture 860z Mezzanine FIO Adapter	21C

Online Firmware Upgrade Utility (Linux x86_64) for HPE Mellanox Ethernet only adapters
Version: 1.0.8 (A) **(Recommended)**
Filename: firmware-nic-mellanox-ethernet-only-1.0.8-2.1.x86_64.compsig; firmware-nic-mellanox-ethernet-only-1.0.8-2.1.x86_64.rpm

Important Note!

Known Issues for FW version 2.42.5000 :

- Enabling/disabling cq_timestamp using mlxconfig is not supported.
- In a card with 2 separate LEDs scheme (a Phy LED and a logic LED) only the Phy LED will lit. Meaning, the orange LES will not be active while the ETH link is in an idle mode.
- In SR-IOV setup, using mlxconfig when the PF is passed through to a VM requires a reboot of the Hypervisor.
- Downgrade to previous GA requires server reboot.Downgrading from v2.30.8000 or later to an earlier version than 2.30.8000 requires

server reboot. Reboot the server.
- On ConnectX-3 Ethernet adapter cards, there is a mismatch between the GUID value returned by firmware management tools and that returned by fabric/driver utilities that read the GUID via device firmware (e.g., using ibstat). Mlxburn/flint return 0xffff as GUID while the utilities return a value derived from the MAC address. For all driver/firmware/software purposes, the lattervalue should be used.
- SBR should be asserted for a minimum of 50 milliseconds for the ConnectX®-3 adapters
- On Pilot1 SL230, PCIe link occasionally does not come up at Gen3 speed
- RH6.3 Inbox driver causes kernel panic when SR-IOV is enabled on VPI cards due to driver compatibility issue.
- In advanced steering mode, side band management connectivity may be lost when having more than 8 QP per mcg.
- When SR-IOV is disabled in the system BIOS, a PCI issue is noticed in Ubuntu v12.04.3 with Linux kernel v3.8 which affects NICs of several manufacturers including Mellanox's, preventing them from operating.
- MFT tools might leave the flash semaphore locked if the tool operation is forced stopped. The locked semaphore prevents the firmware from accessing the flash and causes firmware hang.
- Cable Info MAD reports a wrong cable info when usingthe MC2210411-SR4 module
- Gen2 failure at temperature sweep up to 10C/min (for MT27518A1-FDIR-BV only).
- PCIe Gen2 link unstable at temperature sweep of 10C/min for MT27518A1-FDIR-BV
- Bloom filter is currently not supported.
- Firmware downgrade message When downgrading from firmware v2.11.0000 and using MFT 3.0.0-3
- RM#DMFS should not be enabled when working with InfiniBand on MLNX_OFED-2.0.3
- RM#VPD read-only fields are writable.
- Increasing SymbolErrorCounter When working in VPI mode with port1 FDR and port2 40G, error counters misbehave and increase rapidly
- Setting the device to 128Byte CQ/EQ stride will cause misbehavior of sideband management resulting in communication loss.
- CQ and EQ cannot be configured to different stride sizes.
- ConnectX-3 Pro VF device ID is presented the same as ConnectX-3 VF device ID due to driver limitations.
- RSOD while running PXE (legacy) on G9 servers. This occurs only when PXE boot fails and BIOS boots from HDD. Currently it is pending BIOS fix.
- Changing port protocol from ETH to IB on port with NCSI/IPMI enabled while the port is connected to ETH switch is not supported.
- RDP over IPv6 is currently not functional.
- Sniffer QP cannot be removed from the regular rule after adding the QP with insertion scheme equals to "push to that rule"
- Since only a single Boot Entry Vector (BEV) per PCI Physical Function is supported, disabling the first port causes the second port to disappear as well.
- The NIC does not notify the driver of a link-down incident when a cable is unplugged from a NIC port with 56GbE port link.
- 56GbE link is not raised when using 100GbE optic cables.
- When working with MLNX_OFED v3.3-1.0.0.0, server reboot could get stuck due to a kernel panic in mlx-4_en_get_drvinfo() that is called from asynchronous event handler.
- 832298:When running ibdump, loopback traffic is mirroring into the kernel driver.
- AHS reports wrong MTU size
- RM#846523: MAC address that are set from the OS using ifconfig are not reflected in the OCBB buffer.

Known Issues for FW version 14.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
- Health counter increases every 50ms instead of 10ms.
- mlxconfig tool presents all possible expansion ROM images instead of presenting only the existing images.
- An ethernet multicas loopback packet is not counted (even if it is not local loopback packets)when running the nic_receive_steering_discard command.
- When a dual-port VHCA sends RoCE packets on its non-native port, and the packet arrives to its affiliated vport FDB, a mismatch might happen on the rules that match the packet source vport.

Known Issues for FW version 12.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
- On rare occasions, retransmissions/packet loss under signature can cause error reporting and terminate the connection.
- Health counter increases every 50ms instead of 10ms.
- mlxconfig tool presents all possible expansion ROM images, instead of presenting only the existing images.
- An Ethernet multicast loopback packet is not counted (even if it is not a local loopback packet) when running the nic_receive_steering_discard command.
  When a dual-port VHCA sends a RoCE packet on its non-native port. and the packet arrives to its affiliated vport FDB, a mismatch might happen on the rules that match the packet source vport.
  During DC CNAK stress tests, DC CNAK timeout (CNAK drops) might occur.

Known Issues for FW version 16.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
  Health counter increases every 50ms instead of 10ms.

Prerequisites

HPE Synergy 6410C 25/50Gb Ethernet Adapter (868779-B21) must first be upgraded to prerequisite firmware version 12.21.2808 before updating to 12.22.0148 or 12.22.0194.
12.22.0194 is the first secure firmware for HPE Synergy 6410C 25/50Gb Ethernet Adapter (868779-B21). Once this device is upgraded to firmware 12.22.0194, downgrade is not allowed.

Fixes

Fixes submitted in version 2.42.5000 :

The PortRcvPkts counter was prevented from being cleared after resetting it..

System Time Out on the configuration cycle of the VFs when more than 10 Virtual Functions performed FLR and the completion Time Out value was configured to a range of less than 16 msec.
- The server hung and resulted in NMI (Non-maskable interrupt) when run-ning "mlxfwtop –d mt4103_pci_cr0" while restarting the driver in parallel (from a differ-ent thread). In this case, the downstream bridge over the device reported completion timeout error.
- In flow_steering, BMC could not receive a ping over IPV6 after running bmc_reboot.
- While closing the HCA (Host Channel Adapters), RX packet caused bad access to resources that did not exist, and consequently caused the QPCGW or the irisc to get stuck.
- The master SMLID and the LID was either 0 or 0xFFFF when the port was neither active nor armed.
- ibdump could not capture all MADs packets.
- Link could not go up after reboot.
- A rare issue caused the PCIe configuration cycle that arrived during the time of sw_reset to generate 2 completions.
- NC-SI (Network Controller Sideband Interface) did not work when adding the disable_stat-ic_steering_ini field in the ini file, due to memory allocation issue for this field in the scratchpad.

Fixes submitted in version 14.22.1414 :

- A temperature normalization function calculation issue. Now the cable gain that is not pure integer is taken into account was fixed.
- An issue related to the parser of object 0x8 in ASN that caused different structure in response was fixed.
- Added the option to avoid unintentionally powering off the backplane port cage upon reboot when in standby mode.
- An issue that caused the driver to return a wrong logical OR of the 2 physical ports, when querying the vport state when the LAG was enabled wre fixed.
- Increased the Full Wire Speed (FWS) threshold value to improve EDR link results.
- An issue that resulted in "Destroy LAG" command failure if a VFs received an FLR while its affinity QPs were open.
- When RoCE Dual Port mode is enabled, tcpdump is not functional on the 2nd port.

Enhancements

Firmware for the following devices are updated to 2.42.5000:

779799-B21 (HP Ethernet 10G 2-port 546FLR-SFP+ Adapter)
779793-B21 (HP Ethernet 10G 2-port 546SFP+ Adapter)

New features and changes in version 2.42.5000:

- Added support for the following features:
  - TLV: CX3_GLOBAL_CONF to enable/disable timestamp on incoming packets through mlxconfig configuration.
  - User MAC configuration.
  - Automatically collecting mstdump before driver reset.
  - to detect DEAD_IRISC (plastic) from TPT (iron) and raise an assert.
- Enhanced the debug ability for command timeout cases.
- Added a new field to "set port" command which notifies the firmware what is the user_mtu size.

Firmware for the following devices are updated to 14.22.1414 :

817749-B21 (HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter)
817753-B21 (HPE Ethernet 25Gb 2-port 640SFP28 Adapter)

New features and changes in version 14.22.1414:

- Transition from 4MB to 7M Firmware Image Banks.
- **Software Reset Flow:** Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
- **Steering Discard Packet Counters:** The following counters were added to count the discard packets (per vport)
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow
  - in dual port devices to 20 VFs
  - in single port devices to 58 VFs
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports
- forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Firmware for the following device is updated to 12.22.1414 :

868779-B21 (HPE Synergy 6410C 25/50Gb Ethernet Adapter)

New features and changes in version 12.22.1414:

- Transition from 4MB to 7M Firmware Image Banks.
- **Software Reset Flow:** Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
- **Steering Discard Packet Counters:** The following counters were added to count the discard packets (per vport)
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down

- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow
  - in dual port devices to 20 VFs
  - in single port devices to 58 VFs
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Firmware for the following device is updated to 16.22.1414 :

874253-B21 (HPE Ethernet 100Gb 1-port 842QSFP28 Adapter)

New features and changes in version 16.22.1414:

- Transition from 4MB to 7M Firmware Image Banks.
- **Software Reset Flow:** Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
- **Steering Discard Packet Counters:** The following counters were added to count the discard packets (per vport)
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- Added support for Push/Pop VLAN, new FLOW TABLE ENTRY actions. These new actions are used by the driver to implement Q-in-Q functionality.
- Packet Pacing in ConnectX-5 adapter cards.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Supported Devices and Features

HPE Part Number	InfiniBand Card Type	PSID
779793-B21	HP Ethernet 10Gb 2-port 546SFP+ Adapter	HP_1200111023
779799-B21	HP Ethernet 10Gb 2-port 546FLR-SFP+ Adapter	HP_2240110004
817749-B21	HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter	HP_2690110034
817753-B21	HPE Ethernet 25Gb 2-port 640SFP28 Adapter	HP_2420110034
868779-B21	HPE Synergy 6410C 25/50Gb Ethernet Adapter	HPE0000000006
874253-B21	HPE Ethernet 100Gb 1-port 842QSFP28 Adapter	HPE0000000014

Online Firmware Upgrade Utility (Linux x86_64) for HPE Mellanox IB only ConnectX4 and ConnectX5 devices on Linux x86_64 platform
Version: 1.0.2 **(Recommended)**
Filename: firmware-nic-mellanox-ib-cx4-cx5-1.0.2-1.1.x86_64.compsig; firmware-nic-mellanox-ib-cx4-cx5-1.0.2-1.1.x86_64.rpm

Important Note!

Known Issues in firmware version 12.22.4030 and 16.22.4030:

- The maximum "read" size of MTRC_STDB is limited by 272 Bytes.
- Using vl_arb_high or vl_arb_low simultaneously might cause unexpected behavior in QoS functionality.

Prerequisites

Due to significant firmware changes, the devices mentioned in the table below must be upgraded to the prerequisite version first, then programmed to version 16.22.0194 and onwards.

InfiniBand Card Type	Prerequisite firmware version
HPE Apollo InfiniBand EDR 100Gb 2-port 841z Mezzanine Adapter (872723-B21)	16.21.2808

HPE InfiniBand EDR 100Gb 1-port 841QSFP28 Adapter (872725-B21)	16.21.2808

Fixes

Fixes in firmware version 12.22.4030 and 16.22.4030:

- In rare cases, where the width of the receiver's electrical eye is narrow, the link might raise with BER lower than 10^-12.
- LRO timeout configuration is now taken from the TLV configuration instead of the static defined values.
- Added a filter to ignore module temperature reads below -40C and above 125C.
- Closed the vport as part of the fast teardown flow, to prevent Ack to be sent without been scatter to memory.
- A rare scenario where the PERST# de-assertion arrived at a specific critical time period was handled.
- Temperature normalization function calculation issue. Now the cable gain that is not pure integer is taken into account.
- The parser of object 0x8 in ASN that caused different structure in response.
- An issue that caused MSIX interrupt lost while the HCA performed an FLR was handled.
- An issue that caused a race condition between the firmware boot process and the MSIX access from the PCIe, which resulted in lost writes into the MSIX vector was fixed.

Enhancements

Firmware for the following devices are updated to 12.22.4030:

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter)

New features and changes in version 12.22.4030:

- **AS Notify:** AS Notify enables IBM’s Power CPU architecture to boost performance by allowing the hardware to issue light weight “interrupts” to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.
- **Port Enable:** When set, the device supports emulating link down for all the associated functions using “ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters”.
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.

Firmware for the following devices are updated to 16.22.4030:

879482-B21 (HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter)
872726-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter)

New features and changes in version 16.22.4030:

- **AS Notify:** AS Notify enables IBM’s Power CPU architecture to boost performance by allowing the hardware to issue light weight “interrupts” to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.
- **Port Enable:** When set, the device supports emulating link down for all the associated functions using “ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters”.
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.
- Added support for striding RQ in InfiniBand.
- **QoS "Rate Limit":** Added support to limit the transmission rate of individual InfiniBand port Service Levels. This capability is
- configurable through a new vendor-specific MAD (QosConfigSL).
-
-

Supported Devices and Features

Supported Devices:

HPE Part Number	Device Name	PSID
843400-B21	HPE Apollo A10 InfiniBand EDR (100Gb) 2-port Adapter	HPE2920111032
872723-B21	HPE Apollo InfiniBand EDR 100Gb 2-port 841z Mezzanine Adapter	HPE0000000017
872725-B21	HPE InfiniBand EDR 100Gb 1-port 841QSFP28 Adapter	HPE0000000008

Online Firmware Upgrade Utility (Linux x86_64) for HPE Mellanox VPI (Ethernet and Infiniband mode) ConnectX4 and ConnectX5 devices on Linux x86_64 platform
Version: 1.0.4 **(Recommended)**
Filename: firmware-hca-mellanox-vpi-connectx4-1.0.4-1.1.x86_64.compsig; firmware-hca-mellanox-vpi-connectx4-1.0.4-1.1.x86_64.rpm

Important Note!

Known Issues in firmware version 12.22.4030 and 16.22.4030:

- The maximum "read" size of MTRC_STDB is limited by 272 Bytes.
- Using vl_arb_high or vl_arb_low simultaneously might cause unexpected behavior in QoS functionality.

Prerequisites

Due to significant firmware changes, the devices mentioned in the table below must be upgraded to the prerequisite version first, then programmed to version 16.22.0194 and onwards.
16.22.0194 is the first secure firmware for HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter (879482-B21). Once this device is upgraded to firmware 16.22.0194, downgrade is not allowed.

InfiniBand Card Type	Prerequisite firmware version
HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter (872726-B21)	16.21.2808
HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter (879482-B21)	16.21.2800

Fixes

Fixes in firmware version 12.22.4030 and 16.22.4030:

- In rare cases, where the width of the receiver's electrical eye is narrow, the link might raise with BER lower than 10^-12.
- LRO timeout configuration is now taken from the TLV configuration instead of the static defined values.
- Added a filter to ignore module temperature reads below -40C and above 125C.
- Closed the vport as part of the fast teardown flow, to prevent Ack to be sent without been scatter to memory.
- A rare scenario where the PERST# de-assertion arrived at a specific critical time period was handled.
- Temperature normalization function calculation issue. Now the cable gain that is not pure integer is taken into account.
- The parser of object 0x8 in ASN that caused different structure in response.
- An issue that caused MSIX interrupt lost while the HCA performed an FLR was handled.
- An issue that caused a race condition between the firmware boot process and the MSIX access from the PCIe, which resulted in lost writes into the MSIX vector was fixed.

Enhancements

Firmware for the following devices are updated to 12.22.4030:

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter)

New features and changes in version 12.22.4030:

- **AS Notify:** AS Notify enables IBM's Power CPU architecture to boost performance by allowing the hardware to issue light weight "interrupts" to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.
- **Port Enable:** When set, the device supports emulating link down for all the associated functions using "ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters".
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.

Firmware for the following devices are updated to 16.22.4030:

879482-B21 (HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter)
872726-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter)

New features and changes in version 16.22.4030:

- **AS Notify:** AS Notify enables IBM's Power CPU architecture to boost performance by allowing the hardware to issue light weight "interrupts" to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.
- **Port Enable:** When set, the device supports emulating link down for all the associated functions using "ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters".
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.
- Added support for striding RQ in InfiniBand.
- **QoS "Rate Limit":** Added support to limit the transmission rate of individual InfiniBand port Service Levels. This capability is

configurable through a new vendor-specific MAD (QosConfigSL).

Supported Devices and Features

HPE Part Number	Device Name	PSID
825110-B21	HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter	HP_2180110032
825111-B21	HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter	HP_2190110032
872726-B21	HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter	HPE0000000009
879482-B21	HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter	HPE0000000022

Online Firmware Upgrade Utility (Linux x86_64) for HPE Mellanox VPI (Ethernet and Infiniband mode) devices on Linux x86_64 platform
Version: 1.0.6 **(Recommended)**
Filename: firmware-hca-mellanox-vpi-eth-ib-1.0.6-1.1.x86_64.compsig; firmware-hca-mellanox-vpi-eth-ib-1.0.6-1.1.x86_64.rpm

Important Note!

Known Issues in firmware 2.40.5030, 2.40.5072, 2.42.5000, 2.42.5004:

- Downgrading from v2.30.8000 or later to an earlier version than 2.30.8000 requires server reboot.
  Workaround: Reboot the server.
- On ConnectX-3 Ethernet adapter cards, there is a mismatch between the GUID value returned by firmware management cards tools and that returned by fabric/driver utilities that read the GUID via device firmware (e.g., using ibstat). Mlxburn/flint return 0xffff as GUID while the utilities return a value derived from the MAC address. For all driver/firmware/software purposes, the latter value should be used.
  Workaround: Use the GUID value returned by the fabric/driver utilities (not 0xffffff).
- SBR should be asserted for a minimum of 50 milliseconds for the ConnectX®-3 adapters.
- On Pilot1 SL230, PCIe link occasionally does not come up at Gen3 speed.
- RH6.3 Inbox driver causes kernel panic when SR-IOV is enabled on VPI cards due to driver compatibility issue.
- In advanced steering mode, side band management connectivity may be lost when having more than 8 QP per mcg.
- When SR-IOV is disabled in the system BIOS, a PCI issue is noticed in Ubuntu v12.04.3 with Linux kernel v3.8 which affects NICs of several manufacturers including Mellanox's, preventing them from operating.
  Workaround: Enable SR-IOV in the BIOS.
- MFT tools might leave the flash semaphore locked if the tool operation is forced stopped. The locked semaphore prevents the firmware from accessing the flash and causes firmware hang..
  Workaround: Clear the semaphore using MFT command: flint -clear_semaphore
- Cable Info MAD reports a wrong cable info when using the MC2210411-SR4 module.
- Gen2 failure at temperature sweep up to 10C/min (for MT27518A1-FDIR-BV only).
- PCIe Gen2 link unstable at temperature sweep of 10C/min for MT27518A1-FDIR-BV.
- Bloom filter is currently not supported.
- When downgrading from firmware v2.11.0000 and using MFT 3.0.0-3, Release the following message is displayed due to the mlxconfig tool:
  DMFS steering mode with IB in Linux You are trying to override configurable FW by non-configurable FW. If you continue, old FW configurations will be cleared, do youwant to continue ? (y/n) [n] : y
  You are trying to restore default configuration, do you want to continue ? (y/n) [n] :y
- DMFS should not be enabled when working with InfiniBand on MLNX_OFED-2.0.3.
  Workaround: Upgrade to MLNX_OFED-2.1-x.x.x. or later.
- VPD read-only fields are writable.
  Workaround: Do not write to read- only fields if you wish to preserve them.
- When working in VPI mode with port1 FDR and port2 40G, error counters misbehave and increase rapidly.
- Setting the device to 128Byte CQ/EQ stride will cause misbehavior of sideband management resulting in communication loss.
- CQ and EQ cannot be configured to different stride sizes.
- ConnectX-3 Pro VF device ID is presented the same as.ConnectX-3 VF device ID due to driver limitations.
  Workaround: Use the physical function device ID to identify the device.
- Changing port protocol from ETH to IB on port with NCSI/IPMI enabled while the port is connected to ETH switch is not supported.
  Workaround:
  - Unplug the cable from the switch
  - Restart driver
  - Change the protocol via the appropriate tools.
- RDP over IPv6 is currently not functional.
- **Workaround:** Set the default RoCE mode in the software to RoCE v2 (also when not using RoCE).
  Sniffer QP cannot be removed from the regular rule after adding the QP with insertion scheme equals to "push to that rule".
  Since only a single Boot Entry Vector (BEV) per PCI Physical Function is supported, disabling the first port causes the second port to disappear as well.
- The NIC does not notify the driver of a link-down incident when a cable is unplugged from a NIC port with 56GbE port link.
- 56GbE link is not raised when using 100GbE optic cables.
- When working with MLNX_OFED v3.3-1.0.0.0, server reboot could get stuck due to a kernel panic in mlx4_en_get_drvinfo() that is
- called from asynchronous event handler.
  When running ibdump, loopback traffic is mirroring into the kernel driver.

Known Issues in firmware version 2.42.5000, 2.42.5004:

Enabling/disabling cq_timestamp using mlxconfig is not supported.
In a card with 2 separate LEDs scheme (a Phy LED and a logic LED) only the Phy LED will lit. Meaning, the orange LED will not be active while the ETH link is in an idle mode.
In SR-IOV (Single Root I/O Virtualization) setup, using mlxconfig when the PF (Physical Function) is passed through to a VM (Virtual

Machine) requires a reboot of the Hypervisor.
- Adapter card MCX349A-XCCN may experience longer linkup times of a few seconds with specific switches.
- Adapter card MCX349A-XCCN does not respond to ethtool "identify" command (ethtool -p/--identify).
- MAC address that are set from the OS using ifconfig are not reflected in the OCBB buffer.

Known Issues in firmware version 2.40.5072:

- Ambient sensor does not report via Platform Level Data Model (PLDM) in GEN10 connectX3.

Known Issues in firmware version 2.42.5000:

- MTUSB communication via I2C header on primary I2C bus is supported only in live-fish mode.

Known Issues in firmware version 2.42.5004:

- Cisco bi-directional transceiver is not supported in HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter.

Fixes

Fixes in version 2.40.5030 and 2.40.5072:

- Race between the firmware and the hardware during driver start which blocked outbound completions.
- The firmware did not send link_down event to the driver when running the close_port command.

Fixes in version 2.42.5000:

- PortRcvPkts counter was prevented from being cleared after resetting it.
- The system Timed Out on the configuration cycle of the Virtual Functions (VFs) when more than 10 Virtual Functions performed FLR and the completion Time Out value was configured to a range of less than 16 msec.
- The server hangs and results in NMI when running "mlxfwtop –d mt4103_pci_cr0" while restarting the driver in parallel (from a different thread). In this case, the downstream bridge over the device reported completion timeout error.
- In flow_steering, BMC could not receive a ping over IPV6 after running bmc_reboot.
- While closing the HCA, the RX packet caused bad access to resources that did not exist, and consequently caused the QPCGW or the irisc to get stuck.
- The master SMLID and the LID was either 0 or 0xFFFF when the port was neither active nor armed.
- ibdump could not capture all MADs packets.
- link did not go up after reboot.
- Fixed a rare issue that cause the PCIe configuration cycle that arrived during the time of sw_reset to generate 2 completions.
- Network Controller Sideband Interface (NC-SI) did not work when adding the disable_static_steering_ini field in the ini file, due to memory allocation issue for this field in the scratchpad.

Fixes in version 2.42.5004:

- In UEFI (Unified Extensible Firmware Interface) HII (Human Interface Infrastructure) menu, when using HPE Gen10 devices, both ports appear as port 1.
- In UEFI (Unified Extensible Firmware Interface) boot menu, when using HPE Gen10 devices, the device name appears with an unneeded port number.

Enhancements

Firmware for the following devices are updated to 2.40.5030:
764286-B21
778509-B21

Firmware for the following devices are updated to 2.40.5072:
764285-B21

Firmware for the following devices are updated to 2.42.5004:
764283-B21
764284-B21

Firmware for the following devices are updated to 2.42.5000:
764282-B21

New features in firmware version 2.40.5030:

Added support for the following features.
Temperature thresholds high/low default for MAD sensing and NCSI/IPMI OEM commands.
A new field is added to "set port" command which notifies the firmware what is the user_mtu size.
A protection mechanism which ensures the firmware drops packets which are received in internal Queue Pairs (QPs) and disables the WQE producer fetching.

New features in firmware version 2.40.5072:

Platform Level Data Model (PLDM) support.

New features in firmware version 2.42.5000:

Added support for the following features.
new TLV: CX3_GLOBAL_CONF to enable/disable timestamp on incoming packets through mlxconfig configuration.
User MAC configuration.
Automatically collecting mstdump before driver reset.

A mechanism to detect DEAD_IRISC (plastic) from TPT (iron) and raise an assert.
    - A new field is added to "set port" command which notifies the firmware what is the user_mtu size.
- Improved the debug ability for command timeout cases

Supported Devices and Features

Supported Devices:

HP Part Number	Device Name	PSID
764282-B21	HP InfiniBand QDR/Ethernet 10Gb 2-port 544+M Adapter	HP_1350110023
764283-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M Adapter	HP_1360110017
764284-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter	HP_1370110017
764285-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP Adapter	HP_1380110017
764286-B21	HP InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP Adapter	HP_1390110023
778509-B21	HP Infiniband FDR/Ethernet 10Gb/40Gb 2-port 544+A8L Adapter	HP_2010110021

Online Firmware Upgrade Utility (Windows x64) for HPE Mellanox Ethernet only adapters
Version: 1.0.0.8 (A) **(Recommended)**
Filename: cp036334.compsig; cp036334.exe

Important Note!

Known Issues for FW version 2.42.5000 :

- Enabling/disabling cq_timestamp using mlxconfig is not supported.
- In a card with 2 separate LEDs scheme (a Phy LED and a logic LED) only the Phy LED will lit. Meaning, the orange LES will not be active while the ETH link is in an idle mode.
- In SR-IOV setup, using mlxconfig when the PF is passed through to a VM requires a reboot of the Hypervisor.
- Downgrade to previous GA requires server reboot.Downgrading from v2.30.8000 or later to an earlier version than 2.30.8000 requires server reboot. Reboot the server.
- On ConnectX-3 Ethernet adapter cards, there is a mismatch between the GUID value returned by firmware management tools and that returned by fabric/driver utilities that read the GUID via device firmware (e.g., using ibstat). Mlxburn/flint return 0xffff as GUID while the utilities return a value derived from the MAC address. For all driver/firmware/software purposes, the lattervalue should be used.
- SBR should be asserted for a minimum of 50 milliseconds for the ConnectX®-3 adapters
- On Pilot1 SL230, PCIe link occasionally does not come up at Gen3 speed
- RH6.3 Inbox driver causes kernel panic when SR-IOV is enabled on VPI cards due to driver compatibility issue.
- In advanced steering mode, side band management connectivity may be lost when having more than 8 QP per mcg.
- When SR-IOV is disabled in the system BIOS, a PCI issue is noticed in Ubuntu v12.04.3 with Linux kernel v3.8 which affects NICs of several manufacturers including Mellanox's, preventing them from operating.
- MFT tools might leave the flash semaphore locked if the tool operation is forced stopped. The locked semaphore prevents the firmware from accessing the flash and causes firmware hang.
- Cable Info MAD reports a wrong cable info when usingthe MC2210411-SR4 module
- Gen2 failure at temperature sweep up to 10C/min (for MT27518A1-FDIR-BV only).
- PCIe Gen2 link unstable at temperature sweep of 10C/min for MT27518A1-FDIR-BV
- Bloom filter is currently not supported.
- Firmware downgrade message When downgrading from firmware v2.11.0000 and using MFT 3.0.0-3
- RM#DMFS should not be enabled when working with InfiniBand on MLNX_OFED-2.0.3

- RM#VPD read-only fields are writable.
- Increasing SymbolErrorCounter When working in VPI mode with port1 FDR and port2 40G, error counters misbehave and increase rapidly
- Setting the device to 128Byte CQ/EQ stride will cause misbehavior of sideband management resulting in communication loss.
- CQ and EQ cannot be configured to different stride sizes.
- ConnectX-3 Pro VF device ID is presented the same as ConnectX-3 VF device ID due to driver limitations.
- RSOD while running PXE (legacy) on G9 servers. This occurs only when PXE boot fails and BIOS boots from HDD. Currently it is pending BIOS fix.
- Changing port protocol from ETH to IB on port with NCSI/IPMI enabled while the port is connected to ETH switch is not supported.
- RDP over IPv6 is currently not functional.
- Sniffer QP cannot be removed from the regular rule after adding the QP with insertion scheme equals to "push to that rule"
- Since only a single Boot Entry Vector (BEV) per PCI Physical Function is supported, disabling the first port causes the second port to disappear as well.
- The NIC does not notify the driver of a link-down incident when a cable is unplugged from a NIC port with 56GbE port link.
- 56GbE link is not raised when using 100GbE optic cables.
- When working with MLNX_OFED v3.3-1.0.0.0, server reboot could get stuck due to a kernel panic in mlx-4_en_get_drvinfo() that is called from asynchronous event handler.
- 832298:When running ibdump, loopback traffic is mirroring into the kernel driver.
- AHS reports wrong MTU size
- RM#846523: MAC address that are set from the OS using ifconfig are not reflected in the OCBB buffer.

Known Issues for FW version 14.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
- Health counter increases every 50ms instead of 10ms.
- mlxconfig tool presents all possible expansion ROM images instead of presenting only the existing images.
- An ethernet multicas loopback packet is not counted (even if it is not local loopback packets)when running the nic_receive_steering_discard command.
- When a dual-port VHCA sends RoCE packets on its non-native port, and the packet arrives to its affiliated vport FDB, a mismatch might happen on the rules that match the packet source vport.

Known Issues for FW version 12.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
- On rare occasions, retransmissions/packet loss under signature can cause error reporting and terminate the connection.
- Health counter increases every 50ms instead of 10ms.
- mlxconfig tool presents all possible expansion ROM images, instead of presenting only the existing images.
- An Ethernet multicast loopback packet is not counted (even if it is not a local loopback packet) when running the nic_receive_steering_discard command.
- When a dual-port VHCA sends a RoCE packet on its non-native port. and the packet arrives to its affiliated vport FDB, a mismatch might happen on the rules that match the packet source vport.
- During DC CNAK stress tests, DC CNAK timeout (CNAK drops) might occur.

Known Issues for FW version 16.22.1414 :

- Setting a negative temperature with the hook results in a wrong sensor state report when running the PLDM sensor reading command.
- Health counter increases every 50ms instead of 10ms.

Prerequisites

HPE Synergy 6410C 25/50Gb Ethernet Adapter (868779-B21) must first be upgraded to prerequisite firmware version 12.21.2808 before updating to 12.22.0148 or 12.22.0194.
12.22.0194 is the first secure firmware for HPE Synergy 6410C 25/50Gb Ethernet Adapter (868779-B21). Once this device is upgraded to firmware 12.22.0194, downgrade is not allowed.

Fixes

Fixes submitted in version 2.42.5000 :

- The PortRcvPkts counter was prevented from being cleared after resetting it..
- System Time Out on the configuration cycle of the VFs when more than 10 Virtual Functions performed FLR and the completion Time Out value was configured to a range of less than 16 msec.
- The server hung and resulted in NMI (Non-maskable interrupt) when run-ning "mlxfwtop –d mt4103_pci_cr0" while restarting the driver in parallel (from a differ-ent thread). In this case, the downstream bridge over the device reported completion timeout error.
- In flow_steering, BMC could not receive a ping over IPV6 after running bmc_reboot.
- While closing the HCA (Host Channel Adapters), RX packet caused bad access to resources that did not exist, and consequently caused the QPCGW or the irisc to get stuck.
- The master SMLID and the LID was either 0 or 0xFFFF when the port was neither active nor armed.
- ibdump could not capture all MADs packets.
- Link could not go up after reboot.
- A rare issue caused the PCIe configuration cycle that arrived during the time of sw_reset to generate 2 completions.
- NC-SI (Network Controller Sideband Interface) did not work when adding the disable_stat-ic_steering_ini field in the ini file, due to memory allocation issue for this field in the scratchpad.

Fixes submitted in version 14.22.1414 :

- A temperature normalization function calculation issue. Now the cable gain that is not pure integer is taken into account was fixed.
- An issue related to the parser of object 0x8 in ASN that caused different structure in response was fixed.
- Added the option to avoid unintentionally powering off the backplane port cage upon reboot when in standby mode.
- An issue that caused the driver to return a wrong logical OR of the 2 physical ports, when querying the vport state when the LAG was

enabled wre fixed.
- Increased the Full Wire Speed (FWS) threshold value to improve EDR link results.
- An issue that resulted in "Destroy LAG" command failure if a VFs received an FLR while its affinity QPs were open.
- When RoCE Dual Port mode is enabled, tcpdump is not functional on the 2nd port.

Enhancements

Firmware for the following devices are updated to 2.42.5000:

779799-B21 (HP Ethernet 10G 2-port 546FLR-SFP+ Adapter)
779793-B21 (HP Ethernet 10G 2-port 546SFP+ Adapter)

New features and changes in version 2.42.5000:

- Added support for the following features:
  - TLV: CX3_GLOBAL_CONF to enable/disable timestamp on incoming packets through mlxconfig configuration.
  - User MAC configuration.
  - Automatically collecting mstdump before driver reset.
  - to detect DEAD_IRISC (plastic) from TPT (iron) and raise an assert.
- Enhanced the debug ability for command timeout cases.
- Added a new field to "set port" command which notifies the firmware what is the user_mtu size.

Firmware for the following devices are updated to 14.22.1414 :

817749-B21 (HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter)
817753-B21 (HPE Ethernet 25Gb 2-port 640SFP28 Adapter)

New features and changes in version 14.22.1414:

- Transition from 4MB to 7M Firmware Image Banks.
- **Software Reset Flow:** Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
- **Steering Discard Packet Counters:** The following counters were added to count the discard packets (per vport)
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow
  - in dual port devices to 20 VFs
  - in single port devices to 58 VFs
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Firmware for the following device is updated to 12.22.1414 :

868779-B21 (HPE Synergy 6410C 25/50Gb Ethernet Adapter)

New features and changes in version 12.22.1414:

- Transition from 4MB to 7M Firmware Image Banks.
- **Software Reset Flow:** Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
- **Steering Discard Packet Counters:** The following counters were added to count the discard packets (per vport)
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow
  - in dual port devices to 20 VFs
  - in single port devices to 58 VFs
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Firmware for the following device is updated to 16.22.1414 :

874253-B21 (HPE Ethernet 100Gb 1-port 842QSFP28 Adapter)

New features and changes in version 16.22.1414:

- Transition from 4MB to 7M Firmware Image Banks.

- **Software Reset Flow:** Software detection of a fatal error, automatic creations of an mstdump file for future debug by the software, and resetting of the device.
- **Steering Discard Packet Counters:** The following counters were added to count the discard packets (per vport)
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- Increased the Pause Frame Duration and the XOFF Resend Time to the maximum value defined by the specification.
- **PCI Relax Ordering:** mlxconfig configuration can now enable or disable forced PCI relaxed ordering in mkey_context.
- Added support for Push/Pop VLAN, new FLOW TABLE ENTRY actions. These new actions are used by the driver to implement Q-in-Q functionality.
- Packet Pacing in ConnectX-5 adapter cards.
- **vport Mirroring:** Packets are mirrored based on certain mirroring policy. The policy is set using the "set FTE command" that supports forward action in the ACL tables (ingress/egress).
- **Resiliency: Special Error Event:** Added support for 10GBaseT modules connected to a QSFP cage.
- Accelerated QP's creation time.
- SR-IOV default routing mode is now LID based. The configuration change is available via mlxconfig tool.
- Added PXE and UEFI to additional ConnectX-4 Lx adapter cards. ConnectX-4 Lx now holds PXE, x86-UEFI and Arm-UEFI.

Supported Devices and Features

HPE Part Number	InfiniBand Card Type	PSID
779793-B21	HP Ethernet 10Gb 2-port 546SFP+ Adapter	HP_1200111023
779799-B21	HP Ethernet 10Gb 2-port 546FLR-SFP+ Adapter	HP_2240110004
817749-B21	HPE Ethernet 25Gb 2-port 640FLR-SFP28 Adapter	HP_2690110034
817753-B21	HPE Ethernet 25Gb 2-port 640SFP28 Adapter	HP_2420110034
868779-B21	HPE Synergy 6410C 25/50Gb Ethernet Adapter	HPE0000000006
874253-B21	HPE Ethernet 100Gb 1-port 842QSFP28 Adapter	HPE0000000014

Online Firmware Upgrade Utility (Windows x64) for HPE Mellanox IB only ConnectX4 and ConnectX5 devices on Windows x86_64 platform
Version: 1.0.0.2 **(Recommended)**
Filename: cp034536.compsig; cp034536.exe

Important Note!

Known Issues in firmware version 12.22.4030 and 16.22.4030:

- The maximum "read" size of MTRC_STDB is limited by 272 Bytes.
- Using vl_arb_high or vl_arb_low simultaneously might cause unexpected behavior in QoS functionality.

Prerequisites

Due to significant firmware changes, the devices mentioned in the table below must be upgraded to the prerequisite version first, then programmed to version 16.22.0194 and onwards.

InfiniBand Card Type	Prerequisite firmware version
HPE Apollo InfiniBand EDR 100Gb 2-port 841z Mezzanine Adapter (872723-B21)	16.21.2808
HPE InfiniBand EDR 100Gb 1-port 841QSFP28 Adapter (872725-B21)	16.21.2808

Fixes

Fixes in firmware version 12.22.4030 and 16.22.4030:

- In rare cases, where the width of the receiver's electrical eye is narrow, the link might raise with BER lower than 10^-12.
- LRO timeout configuration is now taken from the TLV configuration instead of the static defined values.
- Added a filter to ignore module temperature reads below -40C and above 125C.
- Closed the vport as part of the fast teardown flow, to prevent Ack to be sent without been scatter to memory.
- A rare scenario where the PERST# de-assertion arrived at a specific critical time period was handled.
- Temperature normalization function calculation issue. Now the cable gain that is not pure integer is taken into account.
- The parser of object 0x8 in ASN that caused different structure in response.
- An issue that caused MSIX interrupt lost while the HCA performed an FLR was handled.
- An issue that caused a race condition between the firmware boot process and the MSIX access from the PCIe, which resulted in lost writes into the MSIX vector was fixed.

Enhancements

Firmware for the following devices are updated to 12.22.4030:

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter)

New features and changes in version 12.22.4030:

- **AS Notify:** AS Notify enables IBM's Power CPU architecture to boost performance by allowing the hardware to issue light weight "interrupts" to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.
- **Port Enable:** When set, the device supports emulating link down for all the associated functions using "ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters".
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.

Firmware for the following devices are updated to 16.22.4030:

879482-B21 (HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter)
872726-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter)

New features and changes in version 16.22.4030:

- **AS Notify:** AS Notify enables IBM's Power CPU architecture to boost performance by allowing the hardware to issue light weight "interrupts" to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.
- **Port Enable:** When set, the device supports emulating link down for all the associated functions using "ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters".
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.
- Added support for striding RQ in InfiniBand.
- **QoS "Rate Limit":** Added support to limit the transmission rate of individual InfiniBand port Service Levels. This capability is configurable through a new vendor-specific MAD (QosConfigSL).

Supported Devices and Features

Supported Devices:

HPE Part Number	Device Name	PSID
843400-B21	HPE Apollo A10 InfiniBand EDR (100Gb) 2-port Adapter	HPE2920111032
872723-B21	HPE Apollo InfiniBand EDR 100Gb 2-port 841z Mezzanine Adapter	HPE0000000017
872725-B21	HPE InfiniBand EDR 100Gb 1-port 841QSFP28 Adapter	HPE0000000008

Online Firmware Upgrade Utility (Windows x64) for HPE Mellanox VPI (Ethernet and Infiniband mode) ConnectX4 and ConnectX5 devices on Windows x86_64 platform
Version: 1.0.0.4 **(Recommended)**
Filename: cp034540.compsig; cp034540.exe

Important Note!

Known Issues in firmware version 12.22.4030 and 16.22.4030:

- The maximum "read" size of MTRC_STDB is limited by 272 Bytes.
- Using vl_arb_high or vl_arb_low simultaneously might cause unexpected behavior in QoS functionality.

Prerequisites

Due to significant firmware changes, the devices mentioned in the table below must be upgraded to the prerequisite version first, then programmed to version 16.22.0194 and onwards.
16.22.0194 is the first secure firmware for HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter (879482-B21). Once this device is upgraded to firmware 16.22.0194, downgrade is not allowed.

InfiniBand Card Type	Prerequisite firmware version
HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter (872726-B21)	16.21.2808
HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter (879482-B21)	16.21.2800

Fixes

Fixes in firmware version 12.22.4030 and 16.22.4030:

- In rare cases, where the width of the receiver's electrical eye is narrow, the link might raise with BER lower than 10^-12.
- LRO timeout configuration is now taken from the TLV configuration instead of the static defined values.
- Added a filter to ignore module temperature reads below -40C and above 125C.
- Closed the vport as part of the fast teardown flow, to prevent Ack to be sent without been scatter to memory.
- A rare scenario where the PERST# de-assertion arrived at a specific critical time period was handled.
- Temperature normalization function calculation issue. Now the cable gain that is not pure integer is taken into account.
- The parser of object 0x8 in ASN that caused different structure in response.
- An issue that caused MSIX interrupt lost while the HCA performed an FLR was handled.
- An issue that caused a race condition between the firmware boot process and the MSIX access from the PCIe, which resulted in lost writes into the MSIX vector was fixed.

Enhancements

Firmware for the following devices are updated to 12.22.4030:

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter)

New features and changes in version 12.22.4030:

- **AS Notify:** AS Notify enables IBM’s Power CPU architecture to boost performance by allowing the hardware to issue light weight “interrupts” to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.
- **Port Enable:** When set, the device supports emulating link down for all the associated functions using “ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters”.
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.

Firmware for the following devices are updated to 16.22.4030:

879482-B21 (HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter)
872726-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter)

New features and changes in version 16.22.4030:

- **AS Notify:** AS Notify enables IBM’s Power CPU architecture to boost performance by allowing the hardware to issue light weight “interrupts” to replace the traditional MSI interrupts.
- **Dump Me Now (DMN):** Dump Me Now (DMN) generated dumps and traces from various components that are crucial for offline debugging. Once an issue is discovered, the dumps can provide useful information about the NIC's state at the time of the failure
- Added support for DSCP mapping on QP RTS2RTS.
- **Port Enable:** When set, the device supports emulating link down for all the associated functions using “ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters”.
- **mlxfwreset:** Reduced and accelerated the mlxfwreset loading time of the firmware update flow.
- **Virtual Functions (VF):** Increased the number of VFs that can work with full VMQoS (8 TC) per PFs as follow:
  - in dual port devices to 20 VFs
  - in single port devices to 64 VFs
- Extended the retry counter (extended_retry_count) to up to 255 instead of 7.
- Added support for striding RQ in InfiniBand.
- **QoS "Rate Limit":** Added support to limit the transmission rate of individual InfiniBand port Service Levels. This capability is configurable through a new vendor-specific MAD (QosConfigSL).

Supported Devices and Features

HPE Part Number	Device Name	PSID
825110-B21	HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28 Adapter	HP_2180110032
825111-B21	HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28 Adapter	HP_2190110032
872726-B21	HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28 Adapter	HPE0000000009
879482-B21	HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter	HPE0000000022

Online Firmware Upgrade Utility (Windows x64) for HPE Mellanox VPI (Ethernet and Infiniband mode) devices on Windows x86_64 platform
Version: 1.0.0.6 **(Recommended)**
Filename: cp033376.compsig; cp033376.exe

Important Note!

Known Issues in firmware 2.40.5030, 2.40.5072, 2.42.5000, 2.42.5004:

- Downgrading from v2.30.8000 or later to an earlier version than 2.30.8000 requires server reboot.
  Workaround: Reboot the server.
- On ConnectX-3 Ethernet adapter cards, there is a mismatch between the GUID value returned by firmware management cards tools and that returned by fabric/driver utilities that read the GUID via device firmware (e.g., using ibstat). Mlxburn/flint return 0xffff as GUID while the utilities return a value derived from the MAC address. For all driver/firmware/software purposes, the latter value should be used.
  Workaround: Use the GUID value returned by the fabric/driver utilities (not 0xfffff).
- SBR should be asserted for a minimum of 50 milliseconds for the ConnectX®-3 adapters.
- On Pilot1 SL230, PCIe link occasionally does not come up at Gen3 speed.
- RH6.3 Inbox driver causes kernel panic when SR-IOV is enabled on VPI cards due to driver compatibility issue.
- In advanced steering mode, side band management connectivity may be lost when having more than 8 QP per mcg.
- When SR-IOV is disabled in the system BIOS, a PCI issue is noticed in Ubuntu v12.04.3 with Linux kernel v3.8 which affects NICs of several manufacturers including Mellanox's, preventing them from operating.
  Workaround: Enable SR-IOV in the BIOS.
- MFT tools might leave the flash semaphore locked if the tool operation is forced stopped. The locked semaphore prevents the firmware from accessing the flash and causes firmware hang..
  Workaround: Clear the semaphore using MFT command: flint -clear_semaphore
- Cable Info MAD reports a wrong cable info when using the MC2210411-SR4 module.
- Gen2 failure at temperature sweep up to 10C/min (for MT27518A1-FDIR-BV only).
- PCIe Gen2 link unstable at temperature sweep of 10C/min for MT27518A1-FDIR-BV.
- Bloom filter is currently not supported.
- When downgrading from firmware v2.11.0000 and using MFT 3.0.0-3, Release the following message is displayed due to the mlxconfig tool:
  DMFS steering mode with IB in Linux You are trying to override configurable FW by non-configurable FW. If you continue, old FW configurations will be cleared, do youwant to continue ? (y/n) [n] : y
  You are trying to restore default configuration, do you want to continue ? (y/n) [n] :y
- DMFS should not be enabled when working with InfiniBand on MLNX_OFED-2.0.3.
  Workaround: Upgrade to MLNX_OFED-2.1-x.x.x. or later.
- VPD read-only fields are writable.
  Workaround: Do not write to read- only fields if you wish to preserve them.
- When working in VPI mode with port1 FDR and port2 40G, error counters misbehave and increase rapidly.
- Setting the device to 128Byte CQ/EQ stride will cause misbehavior of sideband management resulting in communication loss.
- CQ and EQ cannot be configured to different stride sizes.
- ConnectX-3 Pro VF device ID is presented the same as.ConnectX-3 VF device ID due to driver limitations.
  Workaround: Use the physical function device ID to identify the device.
- Changing port protocol from ETH to IB on port with NCSI/IPMI enabled while the port is connected to ETH switch is not supported.
  Workaround:
  - Unplug the cable from the switch
  - Restart driver
  - Change the protocol via the appropriate tools.
- RDP over IPv6 is currently not functional.
  Workaround: Set the default RoCE mode in the software to RoCE v2 (also when not using RoCE).
- Sniffer QP cannot be removed from the regular rule after adding the QP with insertion scheme equals to “push to that rule”.
- Since only a single Boot Entry Vector (BEV) per PCI Physical Function is supported, disabling the first port causes the second port to disappear as well.
- The NIC does not notify the driver of a link-down incident when a cable is unplugged from a NIC port with 56GbE port link.
- 56GbE link is not raised when using 100GbE optic cables.
- When working with MLNX_OFED v3.3-1.0.0.0, server reboot could get stuck due to a kernel panic in mlx4_en_get_drvinfo() that is called from asynchronous event handler.
- When running ibdump, loopback traffic is mirroring into the kernel driver.

Known Issues in firmware version 2.42.5000, 2.42.5004:

- Enabling/disabling cq_timestamp using mlxconfig is not supported.
- In a card with 2 separate LEDs scheme (a Phy LED and a logic LED) only the Phy LED will lit. Meaning, the orange LED will not be active while the ETH link is in an idle mode.
- In SR-IOV (Single Root I/O Virtualization) setup, using mlxconfig when the PF (Physical Function) is passed through to a VM (Virtual Machine) requires a reboot of the Hypervisor.
- Adapter card MCX349A-XCCN may experience longer linkup times of a few seconds with specific switches.
- Adapter card MCX349A-XCCN does not respond to ethtool “identify” command (ethtool -p/--identify).
- MAC address that are set from the OS using ifconfig are not reflected in the OCBB buffer.

Known Issues in firmware version 2.40.5072:

- Ambient sensor does not report via Platform Level Data Model (PLDM) in GEN10 connectX3.

Known Issues in firmware version 2.42.5000:

- MTUSB communication via I2C header on primary I2C bus is supported only in live-fish mode.

Known Issues in firmware version 2.42.5004:

- Cisco bi-directional transceiver is not supported in HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter.

Fixes

Fixes in version 2.40.5030 and 2.40.5072:

- Race between the firmware and the hardware during driver start which blocked outbound completions.

- The firmware did not send link_down event to the driver when running the close_port command.

Fixes in version 2.42.5000:

- PortRcvPkts counter was prevented from being cleared after resetting it.
- The system Timed Out on the configuration cycle of the Virtual Functions (VFs) when more than 10 Virtual Functions performed FLR and the completion Time Out value was configured to a range of less than 16 msec.
- The server hangs and results in NMI when running "mlxfwtop –d mt4103_pci_cr0" while restarting the driver in parallel (from a different thread). In this case, the downstream bridge over the device reported completion timeout error.
- In flow_steering, BMC could not receive a ping over IPV6 after running bmc_reboot.
- While closing the HCA, the RX packet caused bad access to resources that did not exist, and consequently caused the QPCGW or the irisc to get stuck.
- The master SMLID and the LID was either 0 or 0xFFFF when the port was neither active nor armed.
- ibdump could not capture all MADs packets.
- link did not go up after reboot.
- Fixed a rare issue that cause the PCIe configuration cycle that arrived during the time of sw_reset to generate 2 completions.
- Network Controller Sideband Interface (NC-SI) did not work when adding the disable_static_steering_ini field in the ini file, due to memory allocation issue for this field in the scratchpad.

Fixes in version 2.42.5004:

- In UEFI (Unified Extensible Firmware Interface) HII (Human Interface Infrastructure) menu, when using HPE Gen10 devices, both ports appear as port 1.
- In UEFI (Unified Extensible Firmware Interface) boot menu, when using HPE Gen10 devices, the device name appears with an unneeded port number.

Enhancements

Firmware for the following devices are updated to 2.40.5030:
764286-B21
778509-B21

Firmware for the following devices are updated to 2.40.5072:
764285-B21

Firmware for the following devices are updated to 2.42.5004:
764283-B21
764284-B21

Firmware for the following devices are updated to 2.42.5000:
764282-B21

New features in firmware version 2.40.5030:

- Added support for the following features.
  - Temperature thresholds high/low default for MAD sensing and NCSI/IPMI OEM commands.
  - A new field is added to "set port" command which notifies the firmware what is the user_mtu size.
  - A protection mechanism which ensures the firmware drops packets which are received in internal Queue Pairs (QPs) and disables the WQE producer fetching.

New features in firmware version 2.40.5072:

- Platform Level Data Model (PLDM) support.

New features in firmware version 2.42.5000:

- Added support for the following features.
  - new TLV: CX3_GLOBAL_CONF to enable/disable timestamp on incoming packets through mlxconfig configuration.
  - User MAC configuration.
  - Automatically collecting mstdump before driver reset.
  - A mechanism to detect DEAD_IRISC (plastic) from TPT (iron) and raise an assert.
  - A new field is added to "set port" command which notifies the firmware what is the user_mtu size.
- Improved the debug ability for command timeout cases

Supported Devices and Features

Supported Devices:

HP Part Number	Device Name	PSID
764282-B21	HP InfiniBand QDR/Ethernet 10Gb 2-port 544+M Adapter	HP_1350110023

764283-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M Adapter	HP_1360110017
764284-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP Adapter	HP_1370110017
764285-B21	HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP Adapter	HP_1380110017
764286-B21	HP InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP Adapter	HP_1390110023

Firmware - NVDIMM Top

Online Flash Component for Linux - 16GB NVDIMM-N DDR4-2666
Version: 1.04 **(Recommended)**
Filename: RPMS/x86_64/firmware-nvdimm-16gb-1.04-1.1.x86_64.compsig; RPMS/x86_64/firmware-nvdimm-16gb-1.04-1.1.x86_64.rpm

Fixes

Initial release.

Enhancements

Initial release.

Online Flash Component for Windows x64 - 16GB NVDIMM-N DDR4-2666
Version: 1.04 **(Recommended)**
Filename: cp032705.compsig; cp032705.exe

Fixes

Initial relaese.

Enhancements

Initial release.

Firmware - PCIe NVMe Storage Disk Top

Online ROM Flash Component for Windows (x64) - MK000400KWDUK, VK000480KWDUE, MK000800KWDUL, VK000960KWDUF, MK001600KWDUN, and VK001920KWDUH Drives
Version: HPK2 **(Recommended)**
Filename: cp033283.compsig; cp033283.exe; cp033283.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager.**

Fixes

Problems Fixed:

- During HPE ProLiant BL460c Gen10 server boot operation, the drive was not detected by the storage controller.

Enhancements

Enhancements/New Features:

- Enhanced health data retrieval to provide wear status and temperature information.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MK000400KWDUK, VK000480KWDUE, MK000800KWDUL, VK000960KWDUF, MK001600KWDUN, and VK001920KWDUH Drives
Version: HPK2 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-b45e49679c-HPK2-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-b45e49679c-HPK2-1.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager.**

Prerequisites

HPE NVMe PCIe Solid State Drives require below OS versions for online firmware updates:

- Red Hat Enterprise Linux 6.9
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.4
- SUSE Linux Enterprise Server 12 SP3
- SUSE Linux Enterprise Server 11 SP4

Fixes

- Additional improvements in MCTP functionality.
- Drive fails to train in BL460 after Windows warm reset or iLO reset.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MO0400KEFHN, MO0800KEFHP, MO1600KEFHQ, MO2000KEFHR, MT0800KEXUU, and MT1600KEXUV Drives
Version: HPK3 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-2a5b65f157-HPK3-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-2a5b65f157-HPK3-1.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager.**

Prerequisites

HPE NVMe PCIe Solid State Drives require a minimum OS level for online firmware updates:

- Red Hat Enterprise Linux 6.5 or later
- SUSE Linux Enterprise Server 12 or later

Fixes

Problems Fixed:

- HPK3 firmware resolved an issue that caused the disk activity ring, which is located on NVME SSD drive carrier, to constantly spin regardless of drive activity status.

Supplemental Update / Online ROM Flash Component for Linux (x64) - LO0400KEFJQ, LO0800KEFJR, LO1600KEFJT, LO2000KEFJU, LT0800KEXVA, LT1600KEXVB, and LT2000KEXVC Drives
Version: HPK3 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-d64642c780-HPK3-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-d64642c780-HPK3-1.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for**

Proliant and Smart Update Manager.

Prerequisites

HPE NVMe PCIe Solid State Drives require a minimum OS level for online firmware updates:

- Red Hat Enterprise Linux 6.5 or later
- SUSE Linux Enterprise Server 12 or later

Fixes

Problems Fixed:

- HPK3 firmware resolved an issue that caused the disk activity ring, which is located on NVME SSD drive carrier, to constantly spin regardless of drive activity status.

Supplemental Update / Online ROM Flash Component for Linux (x64) - VO0400KEFJB, VO1200KEFJC, and VO2000KEFJD Drives
Version: HPK3 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-9a826ccd8a-HPK3-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-9a826ccd8a-HPK3-1.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager.**

Prerequisites

HPE NVMe PCIe Solid State Drives require a minimum OS level for online firmware updates:

- Red Hat Enterprise Linux 6.5 or later
- SUSE Linux Enterprise Server 12 or later

Fixes

Problems Fixed:

- HPK3 firmware resolved an issue that caused the disk activity ring, which is located on NVME SSD drive carrier, to constantly spin regardless of drive activity status.

Firmware - Power Management Top

Online ROM Flash for Linux - Advanced Power Capping Microcontroller Firmware for HPE Gen10 Servers
Version: 1.0.4 **(Recommended)**
Filename: RPMS/x86_64/firmware-powerpic-gen10-1.0.4-1.1.x86_64.compsig; RPMS/x86_64/firmware-powerpic-gen10-1.0.4-1.1.x86_64.rpm

Important Note!

Important Notes:

None

Deliverable Name:

Advanced Power Capping Microcontroller Firmware for HPE Gen10 Servers

Release Version:

1.0.4

Last Recommended or Critical Revision:

1.0.4

Previous Revision:

1.0.2

Firmware Dependencies:

Integrated Lights-Out 5 (iLO 5) Firmware version 1.15 and System ROM version 1.20 or later

Enhancements/New Features:

Added support for Dynamic Power Capping. For proper operation, please ensure that Integrated Lights-Out 5 (iLO 5) Firmware version 1.15

and System ROM version 1.20 or later are updated on the server.

Problems Fixed:

None

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Linux which is integrated into the standard Linux kernel.

Integrated Lights-Out 5 (iLO 5) Firmware version 1.15 and System ROM version 1.20 or later

Enhancements

Important Notes:

None

Firmware Dependencies:

Integrated Lights-Out 5 (iLO 5) Firmware version 1.15 and System ROM version 1.20 or later

Enhancements/New Features:

Added support for Dynamic Power Capping. For proper operation, please ensure that Integrated Lights-Out 5 (iLO 5) Firmware version 1.15 and System ROM version 1.20 or later are updated on the server.

Known Issues:

None

Online ROM Flash for Linux - Advanced Power Capping Microcontroller Firmware for HPE Gen9 Servers
Version: 1.0.9 (F) **(Optional)**
Filename: RPMS/i386/hp-firmware-powerpic-gen9-1.0.9-6.1.i386.rpm

Important Note!

Important Notes:

Ver. 1.0.9 (F) contains support for new server products. It is functionally equivalent to ver. 1.0.9. It is not necessary to upgrade with Revision F if a previous component revision was used to upgrade the firmware to ver. 1.0.9

Deliverable Name:

Advanced Power Capping Microcontroller Firmware for HPE Gen9 Servers

Release Version:

1.0.9

Last Recommended or Critical Revision:

1.0.7

Previous Revision:

1.0.7

Firmware Dependencies:

None

Enhancements/New Features:

None

Problems Fixed:

Addresses an issue in which the minimum power capping value was incorrectly being calculated on certain systems. This fix increases the accuracy of the minimum capping value set during POST.

Known Issues:

None

Prerequisites

The "HP ProLiant iLO 3/4 Channel Interface Driver" must be installed and running before using this flash component. If the driver is not

running you will receive the following error message:
"The software is not supported for installation on this system.
You must install the iLO Channel Interface driver to use this component."

Fixes

Important Notes:

Ver. 1.0.9 (F) contains support for new server products. It is functionally equivalent to ver. 1.0.9. It is not necessary to upgrade with Revision F if a previous component revision was used to upgrade the firmware to ver. 1.0.9.

Firmware Dependencies:

None

Problems Fixed:

Addresses an issue in which the minimum power capping value was incorrectly being calculated on certain systems. This fix increases the accuracy of the minimum capping value set during POST.

Known Issues:

None

Online ROM Flash for Linux - Power Management Controller
Version: 4.1 (E) **(Recommended)**
Filename: RPMS/i386/hp-firmware-powerpic-dl580-4.1-5.i386.rpm

Important Note!

Important Notes:

Ver. 4.1 (E) contains a change to the Firmware RPM install command name from "cpqsetup" to "hpsetup" and is functionally equivalent to ver. 4.1. It is not necessary to upgrade with Revision E if a previous component revision was used to upgrade the firmware to version 4.1.

Deliverable Name:

Power Management Controller

Release Version:

4.1(E)

Last Recommended or Critical Revision:

This is the initial version of the firmware.

Previous Revision:

This is the initial version of the firmware.

Firmware Dependencies:

None

Enhancements/New Features:

This is the initial version of the firmware.

Problems Fixed:

None

Known Issues:

The smart component prompts for reboot unnecessarily when the installation procedure is completed. Reboot is not required after installation for updates to take effect and hardware stability to be maintained.

Prerequisites

The "HP ProLiant iLO 3/4 Channel Interface Driver" must be installed and running before using this flash component. If the driver is not running you will receive the following error message:
"The software is not supported for installation on this system.
You must install the iLO Channel Interface driver to use this component."

Enhancements

Important Notes:

Ver. 4.1 (E) contains a change to the Firmware RPM install command name from "cpqsetup" to "hpsetup" and is functionally equivalent to ver. 4.1. It is not necessary to upgrade with Revision E if a previous component revision was used to upgrade the firmware to version 4.1.

Firmware Dependencies:

None

Enhancements/New Features:

This is the initial version of the firmware.

Known Issues:

The smart component prompts for reboot unnecessarily when the installation procedure is completed. Reboot is not required after installation for updates to take effect and hardware stability to be maintained.

Online ROM Flash for VMware ESXi - Advanced Power Capping Microcontroller Firmware for HPE Gen9 Servers
Version: 1.0.9 (F) **(Optional)**
Filename: CP031168.zip

Important Note!

Important Notes:

Ver. 1.0.9 (F) contains support for new server products. It is functionally equivalent to ver. 1.0.9. It is not necessary to upgrade with Revision F if a previous component revision was used to upgrade the firmware to ver. 1.0.9

Deliverable Name:

Advanced Power Capping Microcontroller Firmware for HPE Gen9 Servers

Release Version:

1.0.9

Last Recommended or Critical Revision:

1.0.7

Previous Revision:

1.0.7

Firmware Dependencies:

None

Enhancements/New Features:

None

Problems Fixed:

Addresses an issue in which the minimum power capping value was incorrectly being calculated on certain systems. This fix increases the accuracy of the minimum capping value set during POST.

Known Issues:

None

Prerequisites

This component requires that the following HPE drivers be loaded before the component can run.

1. The "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) must be installed and running.

The minimum iLO version for ESXi 5.1, 5.5 and ESXi 6.0 and ESXi 6.5 is 1.4.

2. The "Compaq ROM Utility Driver" (CRU) must be installed and running

The minimum CRU version for ESXi 5.1 is 5.0.3.9.

The minimum CRU version for ESXi 5.5 is 5.5.4.1.

The minimum CRU version for ESXi 6.0 is 6.0.8.

The minimum CRU version for 6.5 is 6.5.8.

Both drivers are integrated into the HPE VMware Custom Image which also contains other HPE advanced management tools. The drivers are also available from the OS specific "HPE Agentless Management Service Offline Bundle" for VMware vSphere 6.5, 6.0, 5.5, and 5.1 on vibsdepot.hpe.com.

Fixes

Important Notes:

Ver. 1.0.9 (F) contains support for new server products. It is functionally equivalent to ver. 1.0.9. It is not necessary to upgrade with Revision F if a previous component revision was used to upgrade the firmware to ver. 1.0.9

Firmware Dependencies:

None

Problems Fixed:

Addresses an issue in which the minimum power capping value was incorrectly being calculated on certain systems. This fix increases the accuracy of the minimum capping value set during POST.

Known Issues:

None

Enhancements

None

Online ROM Flash for VMware ESXi - Power Management Controller
Version: 4.1 (E) **(Recommended)**
Filename: CP026094.zip

Important Note!

Important Notes:

Ver. 4.1 (E) contains updates to the component packaging and is functionally equivalent to ver. 4.1. It is not necessary to upgrade with Revision E if a previous component Revision was used to upgrade the firmware to version 4.1.

Deliverable Name:

Power Management Controller

Release Version:

4.1(E)

Last Recommended or Critical Revision:

This is the initial version of the firmware.

Previous Revision:

This is the initial version of the firmware.

Firmware Dependencies:

None

Enhancements/New Features:

This is the initial version of the firmware.

Problems Fixed:

None

Known Issues:

The smart component prompts for reboot unnecessarily when the installation procedure is completed. Reboot is not required after installation for updates to take effect and hardware stability to be maintained.

Prerequisites

The "HP ProLiant iLO 3/4 Channel Interface Driver" must be installed and running before using this flash component. If the driver is not running you will receive the following error message:
"The software is not supported for installation on this system.
You must install the iLO Channel Interface driver to use this component."

Enhancements

Important Notes:

Ver. 4.1 (E) contains updates to the component packaging and is functionally equivalent to ver. 4.1. It is not necessary to upgrade with Revision E if a previous component Revision was used to upgrade the firmware to version 4.1.

Firmware Dependencies:

None

Enhancements/New Features:

This is the initial version of the firmware.

Known Issues:

The smart component prompts for reboot unnecessarily when the installation procedure is completed. Reboot is not required after installation for updates to take effect and hardware stability to be maintained.

Online ROM Flash for Windows x64 - Advanced Power Capping Microcontroller Firmware for HPE Gen10 Servers
Version: 1.0.4 (B) **(Recommended)**
Filename: cp034430.compsig; cp034430.exe

Important Note!

Important Notes:

Ver. 1.0.4 (B) contains support for new server products. It is functionally equivalent to ver. 1.0.4. It is not necessary to upgrade with Revision (B) if a previous component revision was used to upgrade the firmware to ver. 1.0.4.

Deliverable Name:

Advanced Power Capping Microcontroller Firmware for HPE Gen10 Servers

Release Version:

1.0.4

Last Recommended or Critical Revision:

1.0.4

Previous Revision:

1.0.2

Firmware Dependencies:

Integrated Lights-Out 5 (iLO 5) Firmware version 1.15 and System ROM version 1.20 or later

Enhancements/New Features:

Added support for Dynamic Power Capping. For proper operation, please ensure that Integrated Lights-Out 5 (iLO 5) Firmware version 1.15 and System ROM version 1.20 or later are updated on the server.

Added support for Microsoft Windows 10 (64-bit)

Problems Fixed:

None

Known Issues:

None

Prerequisites

The "iLO 5 Channel Interface Driver" (CHIF) for Windows which is available from Service Pack for ProLiant (SPP).

Integrated Lights-Out 5 (iLO 5) Firmware version 1.15 and System ROM version 1.20 or later.

Enhancements

Important Notes:

Ver. 1.0.4 (B) contains support for new server products. It is functionally equivalent to ver. 1.0.4. It is not necessary to upgrade with Revision (B) if a previous component revision was used to upgrade the firmware to ver. 1.0.4.

Firmware Dependencies:

Integrated Lights-Out 5 (iLO 5) Firmware version 1.15 and System ROM version 1.20 or later

Enhancements/New Features:

Added support for Dynamic Power Capping. For proper operation, please ensure that Integrated Lights-Out 5 (iLO 5) Firmware version 1.15 and System ROM version 1.20 or later are updated on the server.

Added support for Microsoft Windows 10 (64-bit)

Known Issues:

None

Online ROM Flash for Windows x64 - Advanced Power Capping Microcontroller Firmware for HPE Gen9 Servers
Version: 1.0.9 (H) **(Optional)**
Filename: cp034944.exe

Important Note!

Important Notes:

Ver. 1.0.9 (H) contains an update to resolve information disclosure vulnerability issue ref: CVE-2017-8992. It is functionally equivalent to ver. 1.0.9. It is not necessary to upgrade with Revision (H) if a previous component revision was used to upgrade the firmware to ver. 1.0.9.

Deliverable Name:

Advanced Power Capping Microcontroller Firmware for HPE Gen9 Servers

Release Version:

1.0.9

Last Recommended or Critical Revision:

1.0.7

Previous Revision:

1.0.7

Firmware Dependencies:

None

Enhancements/New Features:

Added support for Microsoft Windows 10 (64-bit)

Problems Fixed:

Addressed an issue in which the minimum power capping value was incorrectly being calculated on certain systems. This fix increases the accuracy of the minimum capping value set during POST.

Known Issues:

None

Prerequisites

The "HPE ProLiant iLO 3/4 Channel Interface Driver for Windows" must be installed and running before using this flash component. If the driver is not running you will receive the following error message:
"The software is not supported for installation on this system.
You must install the iLO Channel Interface driver to use this component."

Fixes

Important Notes:

Ver. 1.0.9 (H) contains an update to resolve information disclosure vulnerability issue ref: CVE-2017-8992. It is functionally equivalent to ver. 1.0.9. It is not necessary to upgrade with Revision (H) if a previous component revision was used to upgrade the firmware to ver. 1.0.9.

Firmware Dependencies:

None

Problems Fixed:

Addresses an issue in which the minimum power capping value was incorrectly being calculated on certain systems. This fix increases the accuracy of the minimum capping value set during POST.

Known Issues:

None

Enhancements

Added support for Microsoft Windows 10 (64-bit)

Online ROM Flash for Windows x64 - Power Management Controller
Version: 4.1 (E) **(Recommended)**
Filename: cp035154.exe

Important Note!

Important Notes:

Ver. 4.1 (E) contains an update to resolve information disclosure vulnerability issue ref: CVE-2017-8992. It is functionally equivalent to ver. 4.1. It is not necessary to upgrade with Revision (E) if a previous component revision was used to upgrade the firmware to ver.4.1.

Deliverable Name:

Power Management Controller

Release Version:

4.1(E)

Last Recommended or Critical Revision:

This is the initial version of the firmware.

Previous Revision:
This is the initial version of the firmware.

Firmware Dependencies:

None

Enhancements/New Features:

This is the initial version of the firmware.

Problems Fixed:

None

The smart component prompts for reboot unnecessarily when the installation procedure is completed. Reboot is not required after installation for updates to take effect and hardware stability to be maintained.

Prerequisites

The "HP ProLiant iLO 3/4 Channel Interface Driver for Windows" must be installed and running before using this flash component. If the driver is not running you will receive the following error message:
"The software is not supported for installation on this system.
You must install the iLO Channel Interface driver to use this component."

Enhancements

Important Notes:

Ver. 4.1 (E) contains an update to resolve information disclosure vulnerability issue ref: CVE-2017-8992. It is functionally equivalent to ver. 4.1. It is not necessary to upgrade with Revision (E) if a previous component revision was used to upgrade the firmware to ver.4.1.

Firmware Dependencies:

None

Enhancements/New Features:

This is the initial version of the firmware.

Known Issues:

The smart component prompts for reboot unnecessarily when the installation procedure is completed. Reboot is not required after installation for updates to take effect and hardware stability to be maintained.

Firmware - SAS Storage Disk Top

Online ROM Flash Component for VMware ESXi - EG000300JWBHR Drives
Version: HPD3 (C) **(Recommended)**
Filename: CP036113.compsig; CP036113.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**

- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux,**

Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EG000300JWFVB Drives
Version: HPD2 (B) **(Optional)**
Filename: CP036114.compsig; CP036114.zip

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**

Fixes

- This firmware changes some settings to comply with Microsoft Storage Spaces Certification requirements.

Online ROM Flash Component for VMware ESXi - EG000600JWEBH and EG000300JWEBF Drives
Version: HPD3 (C) **(Recommended)**
Filename: CP036115.compsig; CP036115.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EG000600JWFUV and EG001200JWFVA Drives
Version: HPD3 (B) **(Optional)**
Filename: CP036116.compsig; CP036116.zip

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**

Fixes

- This firmware changes some settings to comply with Microsoft Storage Spaces Certification requirements.

Online ROM Flash Component for VMware ESXi - EG000600JWJNP and EG001200JWJNQ Drives
Version: HPD1 (B) **(Recommended)**
Filename: CP036117.compsig; CP036117.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**

Fixes

- This firmware includes a fix for an issue that could cause timeout errors during certain sequential write corner cases. There is also a fix for slow response time during random write workloads.

Online ROM Flash Component for VMware ESXi - EG001800JWJNR and EG002400JWJNT Drives
Version: HPD1 (B) **(Recommended)**
Filename: CP036119.compsig; CP036119.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**

Fixes

- This firmware includes a fix for an issue that could cause timeout errors during certain sequential write corner cases. There is also a fix for slow response time during random write workloads.

Online ROM Flash Component for VMware ESXi - EG0600JETKA, EG0900JETKB, and EG1200JETKC Drives
Version: HPD6 (C) **(Recommended)**
Filename: CP036123.compsig; CP036123.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EO000400JWDKP,EO000800JWDKQ,EO001600JWDKR,MO000400JWDKU,MO000800JWDKV,MO001600JWDLA and MO003200JWDLB Drives
Version: HPD1 (C) **(Recommended)**
Filename: CP036132.compsig; CP036132.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD1 do not need to update to HPD1(C).**

Fixes

- Removed support of UNMAP command.

Online ROM Flash Component for VMware ESXi - MB2000JFEML and MB4000JFEMN Drives
Version: HPD6 (C) **(Critical)**
Filename: CP036147.compsig; CP036147.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(C).**

Fixes

- Corrects a potential data integrity issue caused by an in process write retry incorrectly starting at the wrong location. This issue was found during supplier ongoing reliability testing.
- The firmware also includes emergency power off improvements.

Online ROM Flash Component for VMware ESXi - MB4000JEQNL and MB6000JEQNN Drives
Version: HPDB (C) **(Recommended)**
Filename: CP036152.compsig; CP036152.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPDB do not need to update to HPDB(C).**

Fixes

- Corrects a potential data integrity issue caused by an in process write retry incorrectly starting at the wrong location. This issue was found during supplier ongoing reliability testing.
- The firmware also includes emergency power off improvements.

Enhancements

Enhancements/New Features

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB6000JEQUV and MB8000JEQVA Drives
Version: HPDB (C) **(Recommended)**
Filename: CP036158.compsig; CP036158.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPDB do not need to update to HPDB(C).**

Fixes

Problems Fixed:

- This firmware improves potential timeouts that could occur during the write error recovery process (causing the drive to internally reset), and corrects possible data mismanagement issues.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB6000JVYZD and MB4000JVYZC Drives
Version: HPD3 (B) **(Recommended)**
Filename: CP036160.compsig; CP036160.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- This firmware has a change that allows the drive to meet the requirements for Microsoft Azure Stack certification. It also includes a fix for an issue that could cause timeout errors during certain sequential write corner cases.

Online ROM Flash Component for VMware ESXi - MM1000JEFRB and MM2000JEFRC Drives
Version: HPD8 (B) **(Optional)**
Filename: CP036167.compsig; CP036167.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD8 do not need to update to HPD8(B).**

Fixes

- This firmware allows the drive to meet the requirements for Azure Stack certification.
- This firmware contains a change to the reported drive serial number in VPD page 80. It will now report the same as is displayed on the drive label. Any removed characters are replaced with blank place holders so the log format will not be changed.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MM1000JFJTH Drives
Version: HPD3 (B) **(Optional)**
Filename: CP036168.compsig; CP036168.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- This firmware allows the drive to meet the requirements for Azure Stack certification.
- This firmware contains a change to the reported drive serial number in VPD page 80. It will now report the same as is displayed on the drive label. Any removed characters are replaced with blank place holders so the log format will not be changed.

Enhancements

Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EG001800JWFVC Drives
Version: HPD2 (C) **(Recommended)**
Filename: CP036118.compsig; CP036118.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(C).**

Fixes

- This firmware update eliminates a data integrity risk when an unaligned WRITE and VERIFY command is sent to a bad sector. During these conditions there is a potential for data intended to be written to disk to fail to be written.

Online ROM Flash Component for VMware ESXi - EG0300FCSPH, EG0450FCSPK, EG0600FCSPL, and EG0900FCSPN Drives
Version: HPD2 (C) **(Recommended)**
Filename: CP036120.compsig; CP036120.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EG0300JEHLV, EG0600JEHMA, EG0900JEHMB, and EG1200JEHMC Drives
Version: HPD5 (D) **(Recommended)**
Filename: CP036121.compsig; CP036121.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD5 do not need to update to HPD5(D).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EG0300JFCKA, EG0600JEMCV, EG0900JFCKB, and EG1200JEMDA Drives
Version: HPD6 (C) **(Recommended)**
Filename: CP036122.compsig; CP036122.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EG1800JEHMD Drive
Version: HPD6 (D) **(Recommended)**
Filename: CP036124.compsig; CP036124.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(D).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EG1800JEMDB Drives
Version: HPD5 (B) **(Recommended)**
Filename: CP036125.compsig; CP036125.zip

Fixes

- This firmware includes a fix for slow performance during sequential write workloads with small queue depth.
- Added FW binary unencrypted.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EG1800JFHMH Drives
Version: HPD7 (B) **(Recommended)**
Filename: CP036126.compsig; CP036126.zip

Fixes

- Added FW binary unencrypted.
- This firmware:
  1) Improves JetStress READ Latency performance
  2) Fixes the cause of internal reboots detected in the MSA system
  3) Removes a vendor unique sense code that the controller does not handle properly
  4) Includes changes to eliminate the cause of a potential hang condition

---

Online ROM Flash Component for VMware ESXi - EH000300JWCPK, EH000600JWCPL, and EH000900JWCPN Drives
Version: HPD3 (C) **(Recommended)**
Filename: CP036128.compsig; CP036128.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EH000600JWCPF and EH000900JWCPH Drives
Version: HPD4 (B) **(Recommended)**
Filename: CP036127.compsig; CP036127.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD4 do not need to update to HPD4(B).**

Fixes

- Added FW binary unencrypted.
- This firmware includes a fix for slow performance during sequential write workloads with small queue depth.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EH0300JDXBA, EH0450JDXBB, and EH0600JDXBC Drives
Version: HPD5 (C) **(Recommended)**
Filename: CP036129.compsig; CP036129.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD5 do not need to update to HPD5(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EH0300JDYTH, EH0450JDYTK, and EH0600JDYTL Drives
Version: HPD6 (D) **(Recommended)**
Filename: CP036130.compsig; CP036130.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(D).**

Fixes

- Added FW binary unencrypted.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - EH0300JEDHC, EH0450JEDHD, and EH0600JEDHE Drives
Version: HPD4 (D) **(Recommended)**

Filename: CP036131.compsig; CP036131.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD4 do not need to update to HPD4(D).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB010000JWAYK and MB008000JWAYH Drives
Version: HPD4 (C) **(Critical)**
Filename: CP036138.compsig; CP036138.zip

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPD4 do not need to update to HPD4(C).**

Fixes

- Firmware corrects potential data integrity issues caused by incomplete cache table updates during unaligned writes, an incorrect write retry start location calculation, and improper media read ranges overlapped with cached writes. These issues were only found during supplier ongoing reliability testing.

Online ROM Flash Component for VMware ESXi - MB1000JVYZL, MB2000JVYZN, MB3000JVYZP, and MB4000JVYZQ Drives
Version: HPD2 (C) **(Recommended)**
Filename: CP036142.compsig; CP036142.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB2000JFDSL and MB4000JFDSN Drives
Version: HPD4 (C) **(Recommended)**
Filename: CP036146.compsig; CP036146.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD4 do not need to update to HPD4(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB2000JFEPA and MB4000JFEPB Drives
Version: HPD5 (C) **(Recommended)**
Filename: CP036148.compsig; CP036148.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD5 do not need to update to HPD5(C).**

Fixes

Problems Fixed:

- This firmware contains a change to prevent occasional command completion times in the 4-5 second window when command is received just as the drive is transitioning from active to Idle A.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB4000JEFNC and MB6000JEFND Drives
Version: HPD9 (C) **(Recommended)**
Filename: CP036151.compsig; CP036151.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD9 do not need to update to HPD9(C).**

Fixes

Problems Fixed:

- This firmware contains a change to prevent a drive reset issue, which may affect performance.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB4000JEXYA and MB6000JEXYB Drives
Version: HPD8 (C) **(Recommended)**
Filename: CP036153.compsig; CP036153.zip

Important Note!

Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.
Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.
Customers who already installed firmware version HPD8 do not need to update to HPD8(C).

Fixes

Problems Fixed:

Fixes a data integrity risk which could occur during 4k or greater unaligned writes while the device incurs a smart trip event. During these conditions there is a potential for data intended to be written directly to disk to fail to be written.
Eliminates a data integrity risk when an unaligned Write and Verify command is sent to a bad sector. During these conditions there is

a potential for data intended to be written to disk to fail to be written.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB6000JVYYV Drives
Version: HPD2 (C) **(Recommended)**
Filename: CP036159.compsig; CP036159.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB8000JFECQ Drives
Version: HPD7 (B) **(Recommended)**
Filename: CP036162.compsig; CP036162.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD7 do not need to update to HPD7(B).**

Fixes

- This firmware includes a fix for slow performance during sequential write workloads with small queue depth.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MO0200JEFNV, MO0400JEFPA, MO0800JEFPB, MO1600JEFPC, EO0200JEFPD, EO0400JEFPE, and EO0800JEFPF Drives
Version: HPD3 (C) **(Recommended)**
Filename: CP036169.compsig; CP036169.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Version: HPD6 (B) **(Recommended)**
Filename: CP036170.compsig; CP036170.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(B).**

Fixes

- Added FW binary unencrypted.

Enhancements

Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - VO0480JFDGT, VO0960JFDGU, VO1920JFDGV, and VO3840JFDHA Drives
Version: HPD6 (C) **(Recommended)**
Filename: CP036175.compsig; CP036175.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(C).**

Fixes

- Added FW binary unencrypted

Enhancements

Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - VO1920JEUQQ Drives
Version: HPD3 (C) **(Recommended)**
Filename: CP036176.compsig; CP036176.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(C).**

Fixes

- Added FW binary unencrypted

Enhancements

Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for Windows (x64) - EG000300JWBHR Drives
Version: HPD3 (B) **(Recommended)**
Filename: cp034350.compsig; cp034350.exe; cp034350.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG000300JWFVB Drives
Version: HPD2 **(Optional)**
Filename: cp035611.compsig; cp035611.exe; cp035611.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manage.**

Fixes

- This firmware changes some settings to comply with Microsoft Storage Spaces Certification requirements.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG000600JWEBH and EG000300JWEBF Drives
Version: HPD3 (B) **(Recommended)**
Filename: cp034292.compsig; cp034292.exe; cp034292.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG000600JWFUV and EG001200JWFVA Drives
Version: HPD3 **(Optional)**
Filename: cp035614.compsig; cp035614.exe; cp035614.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux,**

Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manage.

Fixes

- This firmware changes some settings to comply with Microsoft Storage Spaces Certification requirements.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG000600JWJNP and EG001200JWJNQ Drives
Version: HPD1 **(Recommended)**
Filename: cp035603.compsig; cp035603.exe; cp035603.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**

Fixes

- This firmware includes a fix for an issue that could cause timeout errors during certain sequential write corner cases. There is also a fix for slow response time during random write workloads.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG001800JWFVC Drives
Version: HPD2 (B) **(Recommended)**
Filename: cp035543.compsig; cp035543.exe; cp035543.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG001800JWJNR and EG002400JWJNT Drives
Version: HPD1 **(Recommended)**
Filename: cp035599.compsig; cp035599.exe; cp035599.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**

Fixes

- This firmware includes a fix for an issue that could cause timeout errors during certain sequential write corner cases. There is also a fix for slow response time during random write workloads.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG0300FCSPH, EG0450FCSPK, EG0600FCSPL, and EG0900FCSPN Drives
Version: HPD2 (B) **(Recommended)**
Filename: cp034295.compsig; cp034295.exe; cp034295.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(B).**

Fixes

- Added FW binary unencrypted

Enhancements

Added support for SmartRAID 3154-8e RAID controller.
Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG0300JEHLV, EG0600JEHMA, EG0900JEHMB, and EG1200JEHMC Drives
Version: HPD5 (C) **(Recommended)**
Filename: cp035202.compsig; cp035202.exe; cp035202.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD5 do not need to update to HPD5(C).**

Enhancements

Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG0300JFCKA, EG0600JEMCV, EG0900JFCKB, and EG1200JEMDA Drives
Version: HPD6 (B) **(Recommended)**
Filename: cp034298.compsig; cp034298.exe; cp034298.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for Windows Server 2016 Device Guard.
- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for Windows (x64) - EG0600JETKA, EG0900JETKB, and EG1200JETKC Drives
Version: HPD6 (B) **(Recommended)**
Filename: cp034301.compsig; cp034301.exe; cp034301.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an**

HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG1800JEHMD Drive
Version: HPD6 (C) **(Recommended)**
Filename: cp035203.compsig; cp035203.exe; cp035203.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(C).**

Enhancements

Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG1800JEMDB Drives
Version: HPD5 **(Recommended)**
Filename: cp035863.compsig; cp035863.exe; cp035863.md5

Fixes

- This firmware includes a fix for slow performance during sequential write workloads with small queue depth.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EG1800JFHMH Drives
Version: HPD7 (B) **(Recommended)**
Filename: cp035658.compsig; cp035658.exe; cp035658.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD7 do not need to update to HPD7(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EH000300JWCPK, EH000600JWCPL, and EH000900JWCPN Drives
Version: HPD3 (B) **(Recommended)**
Filename: cp034310.compsig; cp034310.exe; cp034310.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EH000600JWCPF and EH000900JWCPH Drives
Version: HPD4 **(Recommended)**
Filename: cp034307.compsig; cp034307.exe; cp034307.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- Added FW binary unencrypted.
- This firmware includes a fix for slow performance during sequential write workloads with small queue depth.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EH0300JDXBA, EH0450JDXBB, and EH0600JDXBC Drives
Version: HPD5 (B) **(Recommended)**
Filename: cp034313.compsig; cp034313.exe; cp034313.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD5 do not need to update to HPD5(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EH0300JDYTH, EH0450JDYTK, and EH0600JDYTL Drives
Version: HPD6 (C) **(Recommended)**
Filename: cp035240.compsig; cp035240.exe; cp035240.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(C).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EH0300JEDHC, EH0450JEDHD, and EH0600JEDHE Drives
Version: HPD4 (D) **(Recommended)**
Filename: cp034316.compsig; cp034316.exe; cp034316.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD4 do not need to update to HPD4(D).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - EO000400JWDKP,EO000800JWDKQ,EO001600JWDKR,MO000400JWDKU,MO000800JWDKV,MO001600JWDLA and MO003200JWDLB Drives
Version: HPD1 (B) **(Recommended)**
Filename: cp035545.compsig; cp035545.exe; cp035545.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPD1 do not need to update to HPD1(B).**

Enhancements

Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB010000JWAYK and MB008000JWAYH Drives
Version: HPD4 (B) **(Critical)**
Filename: cp035595.compsig; cp035595.exe; cp035595.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPD4 do not need to update to HPD4(B).**

Fixes

- Firmware corrects potential data integrity issues caused by incomplete cache table updates during unaligned writes, an incorrect write retry start location calculation, and improper media read ranges overlapped with cached writes. These issues were only found during supplier ongoing reliability testing.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB1000JVYZL, MB2000JVYZN, MB3000JVYZP, and MB4000JVYZQ Drives
Version: HPD2 (B) **(Recommended)**
Filename: cp035654.compsig; cp035654.exe; cp035654.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB2000JFDSL and MB4000JFDSN Drives
Version: HPD4 (B) **(Recommended)**
Filename: cp035643.compsig; cp035643.exe; cp035643.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD4 do not need to update to HPD4(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB2000JFEML and MB4000JFEMN Drives
Version: HPD6 (B) **(Critical)**
Filename: cp035604.compsig; cp035604.exe; cp035604.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(B).**

Fixes

- Corrects a potential data integrity issue caused by an in process write retry incorrectly starting at the wrong location. This issue was found during supplier ongoing reliability testing.
- The firmware also includes emergency power off improvements.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB2000JFEPA and MB4000JFEPB Drives
Version: HPD5 (B) **(Recommended)**
Filename: cp035644.compsig; cp035644.exe; cp035644.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an**

HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD5 do not need to update to HPD5(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB4000JEFNC and MB6000JEFND Drives
Version: HPD9 (B) **(Recommended)**
Filename: cp035638.compsig; cp035638.exe; cp035638.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD9 do not need to update to HPD9(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB4000JEQNL and MB6000JEQNN Drives
Version: HPDB (B) **(Recommended)**
Filename: cp035636.compsig; cp035636.exe; cp035636.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPDB do not need to update to HPDB(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB4000JEXYA and MB6000JEXYB Drives
Version: HPD8 (B) **(Recommended)**
Filename: cp035653.compsig; cp035653.exe; cp035653.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD8 do not need to update to HPD8(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB6000JEQUV and MB8000JEQVA Drives
Version: HPDB (B) **(Recommended)**
Filename: cp035648.compsig; cp035648.exe; cp035648.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPDB do not need to update to HPDB(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB6000JVYYV Drives
Version: HPD2 (B) **(Recommended)**
Filename: cp035655.compsig; cp035655.exe; cp035655.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB6000JVYZD and MB4000JVYZC Drives
Version: HPD3 **(Recommended)**
Filename: cp035592.compsig; cp035592.exe; cp035592.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**

Fixes

- This firmware has a change that allows the drive to meet the requirements for Microsoft Azure Stack certification. It also includes a fix for an issue that could cause timeout errors during certain sequential write corner cases.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB8000JFECQ Drives
Version: HPD7 **(Recommended)**
Filename: cp035652.compsig; cp035652.exe; cp035652.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**

Fixes

- This firmware includes a fix for slow performance during sequential write workloads with small queue depth.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MM1000JEFRB and MM2000JEFRC Drives
Version: HPD8 **(Optional)**
Filename: cp034562.compsig; cp034562.exe; cp034562.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager.**

Fixes

- This firmware allows the drive to meet the requirements for Azure Stack certification.
- This firmware contains a change to the reported drive serial number in VPD page 80. It will now report the same as is displayed on the drive label. Any removed characters are replaced with blank place holders so the log format will not be changed.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MM1000JFJTH Drives
Version: HPD3 **(Optional)**
Filename: cp034509.compsig; cp034509.exe; cp034509.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**

Fixes

- This firmware allows the drive to meet the requirements for Azure Stack certification.
- This firmware contains a change to the reported drive serial number in VPD page 80. It will now report the same as is displayed on the drive label. Any removed characters are replaced with blank place holders so the log format will not be changed.

Enhancements

Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MO0200JEFNV, MO0400JEFPA, MO0800JEFPB, MO1600JEFPC, EO0200JEFPD, EO0400JEFPE, and EO0800JEFPF Drives
Version: HPD3 (B) **(Recommended)**
Filename: cp034334.compsig; cp034334.exe; cp034334.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MO0400JFFCF, MO0800JFFCH, MO1600JFFCK, and MO3200JFFCL Drives
Version: HPD6 (B) **(Recommended)**
Filename: cp035204.compsig; cp035204.exe; cp035204.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(B).**

Fixes

- Added FW binary unencrypted.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - VO0480JFDGT, VO0960JFDGU, VO1920JFDGV, and VO3840JFDHA Drives
Version: HPD4 (D) **(Recommended)**
Filename: cp034345.compsig; cp034345.exe; cp034345.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager.**
- **Customers who already installed firmware version HPD4 do not need to update to HPD4(D).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - VO1920JEUQQ Drives
Version: HPD3 (B) **(Recommended)**
Filename: cp034349.compsig; cp034349.exe; cp034349.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- Added FW binary unencrypted

Enhancements

Added support for SmartRAID 3154-8e RAID controller.
Added support for Windows Server 2016 Device Guard.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG000300JWBHR Drives
Version: HPD3 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-2e4c61fc63-HPD3-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-2e4c61fc63-HPD3-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG000300JWFVB Drives
Version: HPD2 **(Optional)**
Filename: rpm/RPMS/x86_64/firmware-hdd-c5cd837c29-HPD2-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-c5cd837c29-HPD2-1.1.x86_64.rpm

Fixes

- This firmware changes some settings to comply with Microsoft Storage Spaces Certification requirements.

Enhancements

Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG000600JWEBH and EG000300JWEBF Drives
Version: HPD3 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-aa9e289524-HPD3-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-aa9e289524-HPD3-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG000600JWFUV and EG001200JWFVA Drives
Version: HPD3 **(Optional)**
Filename: rpm/RPMS/x86_64/firmware-hdd-f0c91d2fe3-HPD3-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-f0c91d2fe3-HPD3-1.1.x86_64.rpm

Fixes

- This firmware changes some settings to comply with Microsoft Storage Spaces Certification requirements.

Enhancements

- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG000600JWJNP and EG001200JWJNQ Drives
Version: HPD1 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-bdfb8e99d9-HPD1-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-bdfb8e99d9-HPD1-1.1.x86_64.rpm

Fixes

- This firmware includes a fix for an issue that could cause timeout errors during certain sequential write corner cases. There is also a fix for slow response time during random write workloads.

Enhancements

Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG001800JWJNR and EG002400JWJNT Drives
Version: HPD1 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-b1c9eaf74c-HPD1-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-b1c9eaf74c-HPD1-1.1.x86_64.rpm

Fixes

- This firmware includes a fix for an issue that could cause timeout errors during certain sequential write corner cases. There is also a fix for slow response time during random write workloads.

Enhancements

Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG0600JETKA, EG0900JETKB, and EG1200JETKC Drives
Version: HPD6 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-7505dfb5ae-HPD6-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-7505dfb5ae-HPD6-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EO000400JWDKP,EO000800JWDKQ,EO001600JWDKR,MO000400JWDKU,MO000800JWDKV,MO001600JWDLA and MO003200JWDLB Drives
Version: HPD1 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-5dcf26fa42-HPD1-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-5dcf26fa42-HPD1-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**

Enhancements

Added support for HPE Smart Array P824i-p MR Gen10 controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB6000JVYZD and MB4000JVYZC Drives
Version: HPD3 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-e800e8d3b9-HPD3-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-e800e8d3b9-HPD3-1.1.x86_64.rpm

Fixes

- This firmware has a change that allows the drive to meet the requirements for Microsoft Azure Stack certification. It also includes a fix for an issue that could cause timeout errors during certain sequential write corner cases.

Enhancements

- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MM1000JEFRB and MM2000JEFRC Drives
Version: HPD8 **(Optional)**
Filename: rpm/RPMS/x86_64/firmware-hdd-b04257b77b-HPD8-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-b04257b77b-HPD8-1.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager.**

Fixes

- This firmware allows the drive to meet the requirements for Azure Stack certification.
- This firmware contains a change to the reported drive serial number in VPD page 80. It will now report the same as is displayed on the drive label. Any removed characters are replaced with blank place holders so the log format will not be changed.

Enhancements

- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG001800JWFVC Drives
Version: HPD2 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-693b9a2853-HPD2-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-693b9a2853-HPD2-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG0300FCSPH, EG0450FCSPK, EG0600FCSPL, and EG0900FCSPN Drives
Version: HPD2 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-7c1a1734f9-HPD2-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-7c1a1734f9-HPD2-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG0300JEHLV, EG0600JEHMA, EG0900JEHMB, and EG1200JEHMC Drives
Version: HPD5 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-31f91b8622-HPD5-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-31f91b8622-HPD5-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5(C).**

Enhancements

- Added support for HPE Smart Array P824i-p MR Gen10 controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG0300JFCKA, EG0600JEMCV, EG0900JFCKB, and EG1200JEMDA Drives
Version: HPD6 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-ac3fda26eb-HPD6-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-ac3fda26eb-HPD6-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG1800JEHMD Drive
Version: HPD6 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-8a2c06af48-HPD6-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-8a2c06af48-HPD6-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(C).**

Enhancements

- Added support for HPE Smart Array P824i-p MR Gen10 controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG1800JEMDB Drives
Version: HPD5 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-0a38b25661-HPD5-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-0a38b25661-HPD5-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPD5 do not need to update to HPD5(B).**

Enhancements

Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EG1800JFHMH Drives
Version: HPD7 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-7fc5497116-HPD7-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-7fc5497116-HPD7-1.1.x86_64.rpm

Fixes

- Added FW binary unencrypted.
- This firmware:
  1) Improves JetStress READ Latency performance
  2) Fixes the cause of internal reboots detected in the MSA system
  3) Removes a vendor unique sense code that the controller does not handle properly
  4) Includes changes to eliminate the cause of a potential hang condition

---

Supplemental Update / Online ROM Flash Component for Linux (x64) - EH000300JWCPK, EH000600JWCPL, and EH000900JWCPN Drives
Version: HPD3 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-3d97759111-HPD3-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-3d97759111-HPD3-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EH000600JWCPF and EH000900JWCPH Drives
Version: HPD4 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-a05f29cef3-HPD4-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-a05f29cef3-HPD4-1.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EH0300JDXBA, EH0450JDXBB, and EH0600JDXBC Drives
Version: HPD5 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-1cbab97ff0-HPD5-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-1cbab97ff0-HPD5-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD5 do not need to update to HPD5(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EH0300JDYTH, EH0450JDYTK, and EH0600JDYTL Drives
Version: HPD6 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-b9340d29be-HPD6-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-b9340d29be-HPD6-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(C).**

Fixes

- Added FW binary unencrypted.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - EH0300JEDHC, EH0450JEDHD, and EH0600JEDHE Drives
Version: HPD4 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-8c4a212ff9-HPD4-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-8c4a212ff9-HPD4-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD4 do not need to update to HPD4(c).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB010000JWAYK and MB008000JWAYH Drives
Version: HPD4 (B) **(Critical)**
Filename: rpm/RPMS/x86_64/firmware-hdd-6ec35faf90-HPD4-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-6ec35faf90-HPD4-2.1.x86_64.rpm

Fixes

- Firmware corrects potential data integrity issues caused by incomplete cache table updates during unaligned writes, an incorrect write retry start location calculation, and improper media read ranges overlapped with cached writes. These issues were only found during supplier ongoing reliability testing.

Enhancements

Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB1000JVYZL, MB2000JVYZN, MB3000JVYZP, and MB4000JVYZQ Drives
Version: HPD2 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-b85516c7d2-HPD2-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-b85516c7d2-HPD2-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB2000JFDSL and MB4000JFDSN Drives
Version: HPD4 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-46fc43ab26-HPD4-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-46fc43ab26-HPD4-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPD4 do not need to update to HPD4(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB2000JFEML and MB4000JFEMN Drives
Version: HPD6 (B) **(Critical)**
Filename: rpm/RPMS/x86_64/firmware-hdd-624b75c7e2-HPD6-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-624b75c7e2-HPD6-2.1.x86_64.rpm

Fixes

- Corrects a potential data integrity issue caused by an in process write retry incorrectly starting at the wrong location. This issue was found during supplier ongoing reliability testing.
- The firmware also includes emergency power off improvements.

Enhancements

Added support for HPE Smart Array P824i-p MR Gen10 controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB2000JFEPA and MB4000JFEPB Drives
Version: HPD5 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-326de7c0f2-HPD5-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-326de7c0f2-HPD5-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPD5 do not need to update to HPD5(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB4000JEFNC and MB6000JEFND Drives
Version: HPD9 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-af802bb412-HPD9-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-af802bb412-HPD9-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPD9 do not need to update to HPD9(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB4000JEQNL and MB6000JEQNN Drives
Version: HPDB (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-2cfaac41db-HPDB-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-2cfaac41db-HPDB-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPDB do not need to update to HPDB(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB4000JEXYA and MB6000JEXYB Drives
Version: HPD8 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-0f923833e9-HPD8-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-0f923833e9-HPD8-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD8 do not need to update to HPD8(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB6000JEQUV and MB8000JEQVA Drives
Version: HPDB (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-df22f7effd-HPDB-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-df22f7effd-HPDB-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPDB do not need to update to HPDB(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB6000JVYYV Drives
Version: HPD2 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-0595c2a887-HPD2-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-0595c2a887-HPD2-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD2 do not need to update to HPD2(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB8000JFECQ Drives
Version: HPD7 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-252770cdda-HPD7-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-252770cdda-HPD7-1.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**

Fixes

- This firmware includes a fix for slow performance during sequential write workloads with small queue depth.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MM1000JFJTH Drives
Version: HPD3 **(Optional)**
Filename: rpm/RPMS/x86_64/firmware-hdd-fa46c607d6-HPD3-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-fa46c607d6-HPD3-1.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**

Fixes

- This firmware allows the drive to meet the requirements for Azure Stack certification.
- This firmware contains a change to the reported drive serial number in VPD page 80. It will now report the same as is displayed on the drive label. Any removed characters are replaced with blank place holders so the log format will not be changed.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MO0200JEFNV, MO0400JEFPA, MO0800JEFPB, MO1600JEFPC, EO0200JEFPD, EO0400JEFPE, and EO0800JEFPF Drives
Version: HPD3 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-71af849f3b-HPD3-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-71af849f3b-HPD3-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MO0400JFFCF, MO0800JFFCH, MO1600JFFCK, and MO3200JFFCL Drives
Version: HPD6 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-edf6dcd906-HPD6-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-edf6dcd906-HPD6-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - VO0480JFDGT, VO0960JFDGU, VO1920JFDGV, and VO3840JFDHA Drives
Version: HPD6 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-8ed8893abd-HPD6-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-8ed8893abd-HPD6-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager.**
- **Customers who already installed firmware version HPD6 do not need to update to HPD6(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - VO1920JEUQQ Drives
Version: HPD3 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-5d9e841607-HPD3-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-5d9e841607-HPD3-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPD3 do not need to update to HPD3(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Firmware - SATA Storage Disk Top

Online ROM Flash Component for VMware ESXi - MB002000GWFGH and MB001000GWFGF Drives
Version: HPG3 (B) **(Recommended)**
Filename: CP036135.compsig; CP036135.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG3 do not need to update to HPG3(B).**

Fixes

- This firmware has a change that allows the drive to meet the requirements for Azure Stack certification.

Online ROM Flash Component for VMware ESXi - MB006000GWBXQ and MB008000GWBYL Drives
Version: HPG5 (D) **(Recommended)**
Filename: CP036136.compsig; CP036136.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5(D).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB010000GWAYN and MB008000GWAYL Drives
Version: HPG4 (C) **(Critical)**
Filename: CP036137.compsig; CP036137.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Fixes

- Firmware corrects potential data integrity issues caused by incomplete cache table updates during unaligned writes, an incorrect write retry start location calculation, and improper media read ranges overlapped with cached writes. These issues were only found during supplier ongoing reliability testing.

Online ROM Flash Component for VMware ESXi - MB0500GCEHF, MB1000GCEHH, and MB2000GCEHK Drives
Version: HPGD (L) **(Recommended)**
Filename: CP036139.compsig; CP036139.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPGD do not need to update to HPGD(L).**

Fixes

Problems Fixed:

- After long term use of the HDD, a rare condition might occur following a power cycle where the drive heads may land on areas of the disk containing data, which could potentially cause data loss or mechanical damage. Firmware version HPGD prevents this condition from occurring.

Problems Fixed for HPGD (G):

- Component would fail to install drive firmware for drives present in a system configured with two or more external drive enclosures attached to an HP Host Bus Adapter H22x. The following message would be reported in the component log file - "Device appears more than once in tree". The drive firmware installation failure was not observed in configurations having only one external drive enclosure attached to an HP Host Bus Adapter H22x.

Problems Fixed for HPGD (J):

- When attempting to update drive firmware in a VMware vSphere 6.5 environment, the update would fail and the event was logged as a segmentation fault error.

Enhancements

Enhancements/New Features:

- Added support for VMware vSphere 5.5.
- Added support for UEFI (Universal Extensible Firmware Interface) based servers.
- Added support for HP Dynamic Smart Array B140i Controller.

Enhancements/New Features for HPGD(F):

- Updated the flash engine to standardize logging across all SATA drive components.
- Enhanced logging capability to improve the details provided in the component log file.
- VMware Firmware Smart component packaging has changed from a *.scexe package to a *.zip package, which contains an executable binary that provides enhanced security during installation. The functionality of the VMware Smart Component has not changed.

Enhancements/New Features for HPGD (H):

- Adds support for VMware vSphere 6.5.

Enhancements/New Features for HPGD (K):

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB1000GCWCV, MB2000GCWDA, MB3000GCWDB, and MB4000GCWDC Drives
Version: HPGI (D) **(Recommended)**
Filename: CP036112.compsig; CP036112.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPGI do not need to update to HPGI(D).**

Fixes

- This firmware implements a feature which performs a random seek after 100ms of host inactivity.

Enhancements

Enhancements/New Features:

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB1000GVYZE, MB2000GVYZF, MB3000GVYZH, and MB4000GVYZK Drives
Version: HPG4 (C) **(Recommended)**
Filename: CP036141.compsig; CP036141.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB2000GCVBR, MB3000GCVBT, and MB4000GCVBU Drives
Version: HPG5 (H) **(Recommended)**
Filename: CP036143.compsig; CP036143.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these**

configurations.
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5(H).**

Fixes

Problem Fixed:

- Fixes a rare but potential data integrity error during low 5v drive voltage and specific sequential data streaming conditions, which could result in data written to incorrect sectors.

Problems Fixed for HPG5 (C):

- Component would fail to install drive firmware for drives present in a system configured with two or more external drive enclosures attached to an HP Host Bus Adapter H22x. The following message would be reported in the component log file - "Device appears more than once in tree". The drive firmware installation failure was not observed in configurations having only one external drive enclosure attached to an HP Host Bus Adapter H22x.

Problems Fixed for HPG5 (E):

- When attempting to update drive firmware in a VMware vSphere 6.5 environment, the update would fail and the event was logged as a segmentation fault error.

Enhancements

Enhancements/New Features for HPG5 (B):

- Updated the flash engine to standardize logging across all SATA drive components.
- Enhanced logging capability to improve the details provided in the component log file.
- VMware Firmware Smart component packaging has changed from a *.scexe package to a *.zip package, which contains an executable binary that provides enhanced security during installation. The functionality of the VMware Smart Component has not changed.

Enhancements/New Featuresfor HPG5 (D):

- Adds support for VMware vSphere 6.5.

Enhancements/New Features for HPGD (K):

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB2000GCWLT, MB3000GCWLU, and MB4000GCWLV Drives
Version: HPG4 (E) **(Recommended)**
Filename: CP036144.compsig; CP036144.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(E).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB2000GFEMH and MB4000GFEMK Drives
Version: HPG6 (C) **(Critical)**
Filename: CP036145.compsig; CP036145.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG6 do not need to update to HPG6(C).**

Fixes

- Corrects a potential data integrity issue caused by an in process write retry incorrectly starting at the wrong location. This issue was found during supplier ongoing reliability testing.
- The firmware also corrects settings preservation after a code download, and includes emergency power off improvements.

Online ROM Flash Component for VMware ESXi - MB4000GEQNH and MB6000GEQNK Drives
Version: HPGB (C) **(Recommended)**
Filename: CP036150.compsig; CP036150.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPGB do not need to update to HPGB(C).**

Fixes

- Corrects a potential data integrity issue caused by an in process write retry incorrectly starting at the wrong location. This issue was found during supplier ongoing reliability testing.
- The firmware also corrects settings preservation after a code download, and includes emergency power off improvements.

Enhancements

Enhancements/New Features for HPGB (B):

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MB6000GEQUT and MB8000GEQUU Drives
Version: HPGB (C) **(Critical)**
Filename: CP036155.compsig; CP036155.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPGB do not need to update to HPGB(C).**

Fixes

- Corrects a potential data integrity issue caused by an in process write retry incorrectly starting at the wrong location. This issue was only found during supplier ongoing reliability testing.

Online ROM Flash Component for VMware ESXi - MB6000GVYYU Drives
Version: HPG2 (C) **(Recommended)**
Filename: CP036157.compsig; CP036157.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG2 do not need to update to HPG2(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MK0960GECQK Drives
Version: HPG3 (F) **(Recommended)**
Filename: CP036164.compsig; CP036164.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG3 do not need to update to HPG3(F).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MM1000GEFQV and MM2000GEFRA Drives
Version: HPG5 (D) **(Recommended)**
Filename: CP036165.compsig; CP036165.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5(D).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - MM1000GFJTE Drives
Version: HPG1 (E) **(Recommended)**
Filename: CP036166.compsig; CP036166.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG1 do not need to update to HPG1(E).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - VK000240GWEZB, VK000480GWEZC, VK000960GWEZD, VK001920GWEZE, MK000240GWEZF, MK000480GWEZH, MK000960GWEZK, and MK001920GWHRU Drives
Version: HPG6 (C) **(Recommended)**
Filename: CP036172.compsig; CP036172.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an**

HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG6 do not need to update to HPG6(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - XP0032GEFEN, XP0032GDZME, XP0064GEFEP, and XP0064GDZMF Drives
Version: HPS8 (D) **(Recommended)**
Filename: CP036177.compsig; CP036177.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPS8 do not need to update to HPS8(D).**

Prerequisites

Drive models XP0032GEFEN, XP0032GDZME, XP0064GDZMF, and XP0064GEFEP must have firmware version HPS6 installed prior to updating to firmware version HPS8.

Fixes

Firmware Dependency:

- Drive models XP0032GEFEN, XP0032GDZME, XP0064GDZMF, and XP0064GEFEP must have firmware version HPS6 installed prior to updating to firmware version HPS8.

Problems Fixed:

- HPS8 firmware release resolved a firmware timing issue which occurred during drive long self-test and resulted in a timeout condition that caused the drive to become unrecognized by the system.

Problems Fixed for HPS8 (B):

- When attempting to update drive firmware in a VMware vSphere 6.5 environment, the update would fail and the event was logged as a segmentation fault error.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for VMware ESXi - XP0120GFJSL and XP0240GFJSN Drives
Version: HPS4 (D) **(Recommended)**
Filename: CP036178.compsig; CP036178.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPS4 do not need to update to HPS4(D).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for Windows (x64) - XP0032GEFEN, XP0032GDZME, XP0064GEFEP, and XP0064GDZMF Drives
Version: HPS8 (B) **(Recommended)**
Filename: cp035640.compsig; cp035640.exe; cp035640.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPS8 do not need to update to HPS8(B).**

Prerequisites

Drive models XP0032GEFEN, XP0032GDZME, XP0064GDZMF, and XP0064GEFEP must have firmware version HPS6 installed prior to updating to firmware version HPS8.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB001000GWCBC and MB002000GWCBD Drives
Version: HPG4 (C) **(Recommended)**
Filename: cp035650.compsig; cp035650.exe; cp035650.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB001000GWFWK and MB002000GWFWL Drives
Version: HPG4 (C) **(Recommended)**
Filename: cp035587.compsig; cp035587.exe; cp035587.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB002000GWFGH and MB001000GWFGF Drives
Version: HPG3 **(Optional)**
Filename: cp034198.compsig; cp034198.exe; cp034198.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**

Fixes

- This firmware has a change that allows the drive to meet the requirements for Azure Stack certification.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB006000GWBXQ and MB008000GWBYL Drives
Version: HPG5 (C) **(Recommended)**
Filename: cp035657.compsig; cp035657.exe; cp035657.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5(C).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB010000GWAYN and MB008000GWAYL Drives
Version: HPG4 (B) **(Critical)**
Filename: cp035598.compsig; cp035598.exe; cp035598.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(B).**

Fixes

- Firmware corrects potential data integrity issues caused by incomplete cache table updates during unaligned writes, an incorrect write retry start location calculation, and improper media read ranges overlapped with cached writes. These issues were only found during supplier ongoing reliability testing.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB0500GCEHF, MB1000GCEHH, and MB2000GCEHK Drives
Version: HPGD (F) **(Recommended)**
Filename: cp035631.compsig; cp035631.exe; cp035631.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPGD do not need to update to HPGD(F).**

Enhancements

Enhancements/New Features for HPGD (F):

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB1000GCWCV, MB2000GCWDA, MB3000GCWDB, and MB4000GCWDC Drives
Version: HPGI (B) **(Recommended)**
Filename: cp035628.compsig; cp035628.exe; cp035628.md5

Important Note!

Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPGI do not need to update to HPGI(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB1000GDUNU, MB2000GDUNV, MB3000GDUPA, and MB4000GDUPB Drives
Version: HPG4 (C) **(Recommended)**
Filename: cp035641.compsig; cp035641.exe; cp035641.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB1000GVYZE, MB2000GVYZF, MB3000GVYZH, and MB4000GVYZK Drives
Version: HPG4 (C) **(Recommended)**
Filename: cp035662.compsig; cp035662.exe; cp035662.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB2000GCVBR, MB3000GCVBT, and MB4000GCVBU Drives
Version: HPG5 (E) **(Recommended)**
Filename: cp035633.compsig; cp035633.exe; cp035633.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5(E).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB2000GCWLT, MB3000GCWLU, and MB4000GCWLV Drives
Version: HPG4 (C) **(Recommended)**
Filename: cp035642.compsig; cp035642.exe; cp035642.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB2000GFEMH and MB4000GFEMK Drives
Version: HPG6 (B) **(Critical)**
Filename: cp035551.compsig; cp035551.exe; cp035551.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPG6 do not need to update to HPG6(B).**

Fixes

- Corrects a potential data integrity issue caused by an in process write retry incorrectly starting at the wrong location. This issue was found during supplier ongoing reliability testing.
- The firmware also corrects settings preservation after a code download, and includes emergency power off improvements.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB4000GEFNA and MB6000GEFNB Drives
Version: HPG6 (C) **(Recommended)**
Filename: cp035700.compsig; cp035700.exe; cp035700.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG6 do not need to update to HPG6(C).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB4000GEQNH and MB6000GEQNK Drives
Version: HPGB (B) **(Recommended)**
Filename: cp035637.compsig; cp035637.exe; cp035637.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPGB do not need to update to HPGB(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB6000GEBTP Drives
Version: HPG4 (B) **(Recommended)**
Filename: cp035665.compsig; cp035665.exe; cp035665.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB6000GEQUT and MB8000GEQUU Drives
Version: HPGB **(Critical)**
Filename: cp035608.compsig; cp035608.exe; cp035608.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**

Fixes

- Corrects a potential data integrity issue caused by an in process write retry incorrectly starting at the wrong location. This issue was only found during supplier ongoing reliability testing.

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB6000GEXXV Drives
Version: HPG2 (C) **(Recommended)**
Filename: cp035645.compsig; cp035645.exe; cp035645.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG2 do not need to update to HPG2(C).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB6000GVYYU Drives
Version: HPG2 (B) **(Recommended)**
Filename: cp035664.compsig; cp035664.exe; cp035664.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG2 do not need to update to HPG2(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MB8000GFECR Drives
Version: HPG5 (B) **(Recommended)**
Filename: cp035724.compsig; cp035724.exe; cp035724.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MK0960GECQK Drives
Version: HPG3 (E) **(Recommended)**
Filename: cp034319.compsig; cp034319.exe; cp034319.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG3 do not need to update to HPG3(E).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - MM1000GEFQV and MM2000GEFRA Drives
Version: HPG5 (B) **(Recommended)**
Filename: cp034322.compsig; cp034322.exe; cp034322.md5

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager.**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5 (B).**

Fixes

- Added FW binary unencrypted

Enhancements

-
- Added support for Windows Server 2016 Device Guard.
- Added support for SmartRAID 3154-8e RAID controller.
-

Online ROM Flash Component for Windows (x64) - MM1000GFJTE Drives
Version: HPG1 (C) **(Recommended)**

Filename: cp034325.compsig; cp034325.exe; cp034325.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG1 do not need to update to HPG1(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - VK000240GWEZB, VK000480GWEZC, VK000960GWEZD, VK001920GWEZE, MK000240GWEZF, MK000480GWEZH, MK000960GWEZK, and MK001920GWHRU Drives
Version: HPG6 (B) **(Recommended)**
Filename: cp035660.compsig; cp035660.exe; cp035660.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPDG6 do not need to update to HPG6(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - VK0120GFDKE, VK0240GFDKF, VK0480GFDKH, VK0960GFDKK, VK1920GFDKL, and VK3840GFDKN Drives
Version: HPG1 (B) **(Recommended)**
Filename: cp034340.compsig; cp034340.exe; cp034340.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG1 do not need to update to HPG1(B).**

Fixes

- Added FW binary unencrypted

Enhancements

Added support for Windows Server 2016 Device Guard.

Online ROM Flash Component for Windows (x64) - VK0240GEPQN, VK0480GEPQP, and VK0960GEPQQ Drives
Version: HPG1 (B) **(Recommended)**
Filename: cp034343.compsig; cp034343.exe; cp034343.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**

- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG1 do not need to update to HPG1(B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for Windows Server 2016 Device Guard.
- Added support for SmartRAID 3154-8e RAID controller.

Online ROM Flash Component for Windows (x64) - XP0120GFJSL and XP0240GFJSN Drives
Version: HPS4 (B) **(Recommended)**
Filename: cp035649.compsig; cp035649.exe; cp035649.md5

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPS4 do not need to update to HPS4(B).**

Enhancements

- Added support for Windows Server 2016 Device Guard.

Supplemental Update / Online ROM Flash Component for ESXi - MB001000GWCBC and MB002000GWCBD Drives
Version: HPG4 (C) **(Recommended)**
Filename: CP036133.compsig; CP036133.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Fixes

Problems Fixed:

- This firmware corrects a potential issue where the data in the reserved tracks is not properly updated, eliminating the risk of a drive not finishing the boot process on power up.
- Other maintenance fixes and updates are also included with the new firmware.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Supplemental Update / Online ROM Flash Component for ESXi - MB001000GWFWK and MB002000GWFWL Drives
Version: HPG4 (C) **(Recommended)**
Filename: CP036134.compsig; CP036134.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Firmware version HPG4 is designed to prevent any previous firmware revisions from being loaded onto the drive, after the drive is upgraded to HPG4 firmware.

Supplemental Update / Online ROM Flash Component for ESXi - MB1000GDUNU, MB2000GDUNV, MB3000GDUPA, and MB4000GDUPB Drives
Version: HPG4 (E) **(Recommended)**
Filename: CP036140.compsig; CP036140.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(E).**

Fixes

Problems Fixed:

- Reliability enhancement for applications that write data to a narrow range of tracks.

Problems Fixed for HPG4 (C):

- When attempting to update drive firmware in a VMware vSphere 6.5 environment, the update would fail and the event was logged as a segmentation fault error.

Known Issues:

- Firmware cannot be downgraded to HPG3 after updating to HPG4.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Supplemental Update / Online ROM Flash Component for ESXi - MB4000GEFNA and MB6000GEFNB Drives
Version: HPG6 (C) **(Recommended)**
Filename: CP036149.compsig; CP036149.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG6 do not need to update to HPG6(C).**

Fixes

Problems Fixed:

- HPG6 firmware improves drive reliability where disk drives are exposed to long periods of host inactivity which exceed 1 second.

Enhancements

Enhancements/New Features for HPG6 (B):

- Added support for SmartRAID 3154-8e RAID controller.

Supplemental Update / Online ROM Flash Component for ESXi - MB6000GEBTP Drives
Version: HPG4 (C) **(Recommended)**
Filename: CP036154.compsig; CP036154.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**

- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Supplemental Update / Online ROM Flash Component for ESXi - MB6000GEXXV Drives
Version: HPG2 (E) **(Recommended)**
Filename: CP036156.compsig; CP036156.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG2 do not need to update to HPG2(E).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Supplemental Update / Online ROM Flash Component for ESXi - MB8000GFECR Drives
Version: HPG5 (B) **(Recommended)**
Filename: CP036161.compsig; CP036161.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.

Supplemental Update / Online ROM Flash Component for ESXi - VK0120GFDKE, VK0240GFDKF, VK0480GFDKH, VK0960GFDKK, VK1920GFDKL, and VK3840GFDKN Drives
Version: HPG1 (D) **(Recommended)**
Filename: CP036173.compsig; CP036173.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG1 do not need to update to HPG1(D).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
-

Supplemental Update / Online ROM Flash Component for ESXi - VK0240GEPQN, VK0480GEPQP, and VK0960GEPQQ Drives
Version: HPG1 (D) **(Recommended)**

Filename: CP036174.compsig; CP036174.zip

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG1 do not need to update to HPG1(D).**

Fixes

- Added FW binary unencrypted

Enhancements

Added support for SmartRAID 3154-8e RAID controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB001000GWCBC and MB002000GWCBD Drives
Version: HPG4 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-68b12e54d2-HPG4-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-68b12e54d2-HPG4-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(c).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB001000GWFWK and MB002000GWFWL Drives
Version: HPG4 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-bfc4af697b-HPG4-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-bfc4af697b-HPG4-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB002000GWFGH and MB001000GWFGF Drives
Version: HPG3 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-0b575b5895-HPG3-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-0b575b5895-HPG3-1.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an**
- **HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux,**
- **Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**

Fixes

- This firmware has a change that allows the drive to meet the requirements for Azure Stack certification.

Enhancements

- Added support for HPE Smart Array P824i-p MR Gen10 controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB006000GWBXQ and MB008000GWBYL Drives
Version: HPG5 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-a1fd19f9ca-HPG5-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-a1fd19f9ca-HPG5-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB010000GWAYN and MB008000GWAYL Drives
Version: HPG4 (B) **(Critical)**
Filename: rpm/RPMS/x86_64/firmware-hdd-cc819d4bff-HPG4-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-cc819d4bff-HPG4-2.1.x86_64.rpm

Fixes

- Firmware corrects potential data integrity issues caused by incomplete cache table updates during unaligned writes, an incorrect write retry start location calculation, and improper media read ranges overlapped with cached writes. These issues were only found during supplier ongoing reliability testing.

Enhancements

Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB0500GCEHF, MB1000GCEHH, and MB2000GCEHK Drives
Version: HPGD (F) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-b583d96f94-HPGD-6.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-b583d96f94-HPGD-6.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPGD do not need to update to HPGD(F).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB1000GCWCV, MB2000GCWDA, MB3000GCWDB, and MB4000GCWDC Drives
Version: HPGI (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-a1b08f8a6b-HPGI-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-a1b08f8a6b-HPGI-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPGI do not need to update to HPGI(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB1000GDUNU, MB2000GDUNV, MB3000GDUPA, and MB4000GDUPB Drives
Version: HPG4 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-3ab4c70e64-HPG4-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-3ab4c70e64-HPG4-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB1000GVYZE, MB2000GVYZF, MB3000GVYZH, and MB4000GVYZK Drives
Version: HPG4 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-0a7010918e-HPG4-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-0a7010918e-HPG4-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB2000GCVBR, MB3000GCVBT, and MB4000GCVBU Drives
Version: HPG5 (D) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-e4f5b5c9a7-HPG5-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-e4f5b5c9a7-HPG5-4.1.x86_64.rpm

Fixes

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5(D).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB2000GCWLT, MB3000GCWLU, and MB4000GCWLV Drives
Version: HPG4 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-2e70ce7412-HPG4-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-2e70ce7412-HPG4-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB2000GFEMH and MB4000GFEMK Drives
Version: HPG6 (B) **(Critical)**
Filename: rpm/RPMS/x86_64/firmware-hdd-70e3962f98-HPG6-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-70e3962f98-HPG6-2.1.x86_64.rpm

Fixes

- Corrects a potential data integrity issue caused by an in process write retry incorrectly starting at the wrong location. This issue was found during supplier ongoing reliability testing.
- The firmware also corrects settings preservation after a code download, and includes emergency power off improvements.

Enhancements

Added support for HPE Smart Array P824i-p MR Gen10 controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB4000GEFNA and MB6000GEFNB Drives
Version: HPG6 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-40277d55d3-HPG6-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-40277d55d3-HPG6-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPG6 do not need to update to HPG6(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB4000GEQNH and MB6000GEQNK Drives
Version: HPGB (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-bfc95f0628-HPGB-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-bfc95f0628-HPGB-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPGB do not need to update to HPGB(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB6000GEBTP Drives
Version: HPG4 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-3243fce9a0-HPG4-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-3243fce9a0-HPG4-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG4 do not need to update to HPG4(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB6000GEQUT and MB8000GEQUU Drives
Version: HPGB **(Critical)**
Filename: rpm/RPMS/x86_64/firmware-hdd-1d7f19120b-HPGB-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-1d7f19120b-HPGB-1.1.x86_64.rpm

Fixes

- Corrects a potential data integrity issue caused by an in process write retry incorrectly starting at the wrong location. This issue was only found during supplier ongoing reliability testing.

Enhancements

Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB6000GEXXV Drives
Version: HPG2 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-a629fcea59-HPG2-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-a629fcea59-HPG2-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPG2 do not need to update to HPG2(C).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB6000GVYYU Drives
Version: HPG2 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-bdc37cb37f-HPG2-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-bdc37cb37f-HPG2-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG2 do not need to update to HPG2(B).**

Enhancements

Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MB8000GFECR Drives
Version: HPG5 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-6d922fc9a8-HPG5-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-6d922fc9a8-HPG5-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5(B).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MK0960GECQK Drives
Version: HPG3 (D) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-3e34285be7-HPG3-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-3e34285be7-HPG3-4.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG3 do not need to update to HPG3(D).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MM1000GEFQV and MM2000GEFRA Drives
Version: HPG5 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-ec908c3650-HPG5-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-ec908c3650-HPG5-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager.**
- **Customers who already installed firmware version HPG5 do not need to update to HPG5 (B).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - MM1000GFJTE Drives

Version: HPG1 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-95af9a555e-HPG1-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-95af9a555e-HPG1-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG1 do not need to update to HPG1(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - VK000240GWEZB, VK000480GWEZC, VK000960GWEZD, VK001920GWEZE, MK000240GWEZF, MK000480GWEZH, MK000960GWEZK, and MK001920GWHRU Drives
Version: HPG6 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-3db7640485-HPG6-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-3db7640485-HPG6-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**

Fixes

- Firmware improves a NAND threshold level to strengthen differentiation of NAND states to mitigate excessive reallocation of NAND Blocks (Grown Bad Blocks). For important information about this resolved issue, refer to HPE Customer Bulletin a00027721.

Enhancements

Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - VK0120GFDKE, VK0240GFDKF, VK0480GFDKH, VK0960GFDKK, VK1920GFDKL, and VK3840GFDKN Drives
Version: HPG1 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-a2d4b5c742-HPG1-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-a2d4b5c742-HPG1-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG1 do not need to update to HPG1(C).**

Fixes

- Added FW binary unencrypted

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - VK0240GEPQN, VK0480GEPQP, and VK0960GEPQQ Drives
Version: HPG1 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-1a516522d1-HPG1-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-1a516522d1-HPG1-2.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPG1 do not need to update to HPG1(B).**

Fixes

- Added FW binary unencrypted

Supplemental Update / Online ROM Flash Component for Linux (x64) - XP0032GEFEN, XP0032GDZME, XP0064GEFEP, and XP0064GDZMF Drives
Version: HPS8 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-f286f98973-HPS8-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-f286f98973-HPS8-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to a Smart Array controller running in Zero Memory (ZM) mode or a ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the Service Pack for Proliant and Smart Update Manager**
- **Customers who already installed firmware version HPS8 do not need to update to HPS8(C).**

Prerequisites

Drive models XP0032GEFEN, XP0032GDZME, XP0064GDZMF, and XP0064GEFEP must have firmware version HPS5 installed prior to updating to firmware version HPS8.

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - XP0120GFJSL and XP0240GFJSN Drives
Version: HPS4 (C) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-hdd-d355375539-HPS4-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-d355375539-HPS4-3.1.x86_64.rpm

Important Note!

- **Online firmware flashing of drives attached to an HPE Smart Array controller running in Zero Memory (ZM) mode or an HPE ProLiant host bus adapter (HBA) is NOT supported. Only offline firmware flashing of drives is supported for these configurations.**
- **Online drive firmware update available for Smart Array Controllers configured in systems running supported Linux, Microsoft Windows, and VMware environments. All other OSes would require an offline update using the SPP and HP SUM.**
- **Customers who already installed firmware version HPS4 do not need to update to HPS4(c).**

Enhancements

- Added support for SmartRAID 3154-8e RAID controller.
- Added support for HPE Smart Array P824i-p MR Gen10 Controller.

Firmware - Storage Controller Top

Online ROM Flash Component for Linux - HPE Host Bus Adapters H221
Version: 15.10.10.00 (B) **(Optional)**
Filename: rpm/RPMS/i386/firmware-43d7eff89e-15.10.10.00-2.1.i386.rpm

Important Note!

This driver component supports Gen9 servers only with H221 controllers and the controller does not support connection to D2600, D2700,

and D6000 Disk Enclosures with Gen9 servers.

Fixes

Fixes an issue where the appropriate FW version for the Host Bus Adapter (HBA) Stockade (H2xx) driver will not install when using the Service Pack ProLiant (SPP)

Supported Devices and Features

This driver component supports Gen9 servers only with H221 controllers and the controller does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

Online ROM Flash Component for Linux (x64) – HPE Apollo 2000 Gen10 Backplane Expander Firmware
Version: 1.00 **(Optional)**
Filename: rpm/RPMS/x86_64/firmware-smartarray-9f082dffb4-1.00-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-smartarray-9f082dffb4-1.00-1.1.x86_64.rpm

Enhancements

Initial Release

Online ROM Flash Component for Linux (x64) - HPE Apollo 2000 System - SAS Expander
Version: 1.00 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-smartarray-3bf7ece88e-1.00-2.1.x86_64.rpm

Important Note!

- Customers who already installed firmware version 1.00 do not need to update to 1.00 (B).

Enhancements

- Improved integration with Smart Update Manager.

  Note: Upgrading to version 1.00(B) is not necessary if the Apollo 2000 SAS Expander was previously updated to version 1.00.

Online ROM Flash Component for Linux (x64) – HPE Apollo 4200 Gen9 Backplane Expander Firmware
Version: 1.50 (B) **(Optional)**
Filename: rpm/RPMS/x86_64/firmware-smartarray-f18fdefd0b-1.50-2.1.x86_64.rpm

Important Note!

- Power cycle / cold reboot is required if firmware is upgraded from version 1.03 or earlier.

Enhancements

- Enhanced debug capabilities

Online ROM Flash Component for Linux (x64) – HPE SAS Expander Firmware for HPE D2500sb Storage Blade
Version: 2.00 **(Optional)**
Filename: rpm/RPMS/x86_64/firmware-smartarray-1d0696d939-2.00-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-smartarray-1d0696d939-2.00-1.1.x86_64.rpm

Enhancements

Initial Release

Online ROM Flash Component for Linux (x64) - HPE Smart Array P824i-p MR Gen10
Version: 24.23.0-0019 **(Optional)**
Filename: CP033970.md5; CP033970.scexe; deb/firmware-cafee9b6e4_24.23.0.0019-1.1_amd64.deb; rpm/RPMS/x86_64/firmware-cafee9b6e4-24.23.0_0019-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-cafee9b6e4-24.23.0_0019-1.1.x86_64.rpm

Enhancements

- Initial Release

Online ROM Flash Component for VMware ESXi – HPE 12Gb/s SAS Expander Firmware for HPE Smart Array Controllers and HPE HBA Controllers
Version: 4.02 **(Optional)**
Filename: CP033904.compsig; CP033904.zip

Important Note!

- Power cycle / cold reboot is required if firmware is upgraded from version 1.31 or earlier.

Fixes

- Changed the Enclosure's Target and LUN address to the appropriate unique values. Previously these addresses would conflict with the SATA drive in bay #1 which interfered with software defined storage solutions such as Storage Spaces Direct.

Online ROM Flash Component for VMware ESXi – HPE Apollo 2000 System - SAS Expander
Version: 1.00 (B) **(Recommended)**
Filename: CP031314.compsig; CP031314.zip

Important Note!

- **Customers who already installed firmware version 1.00 do not need to update to 1.00 (B).**

Enhancements

- Added support for the VMware vSphere 2016 OS.
- Improved integration with Smart Update Manager.
  Note: Upgrading to version 1.00(B) is not necessary if the Apollo 2000 SAS Expander was previously updated to version 1.00.

Online ROM Flash Component for VMware ESXi – HPE Apollo 4200 Gen9 Backplane Expander Firmware
Version: 1.50 (B) **(Optional)**
Filename: CP036095.zip

Important Note!

- Power cycle / cold reboot is required if firmware is upgraded from version 1.03 or earlier.

Enhancements

- Enhanced debug capabilities

Online ROM Flash Component for VMware ESXi – HPE Apollo 45xx Gen9 Backplane Expander Firmware
Version: 2.08 **(Optional)**
Filename: CP031316.zip

Important Note!

- Please un-plug and re-plug the power cord to the server for firmware upgrade from version 1.03 or earlier to take effect.

Enhancements

- Enhanced debug capabilities.
- Added support for the VMware vSphere 2016 OS.
- Improved integration with Smart Update Manager.

Online ROM Flash component for VMware ESXi - HPE Dual 8GB microSD USB
Version: 1.3.2.215 **(Recommended)**
Filename: CP034825.compsig; CP034825.zip

Fixes

- To show corresponding HPE Dual 8GB Micron SD part number in Agentless Management Service version 11.2.0 or later.

Online ROM Flash Component for VMware ESXi - HPE Express Bay Enablement Switch Card
Version: 1.78 **(Optional)**
Filename: CP033861.zip

Important Note!

- Power cycle / cold reboot is required after installation for updates to take effect.

Prerequisites

- The HP ProLiant iLO firmware version must be v2.20 or later. If the HP ProLiant iLO firmware is older than v2.20 you will receive the

following error message:

Check dependency failed.

Current version: iLOx x.xx

Minimum version required: iLO4 2.20

The software will not be installed on this system because the required hardware is not present in the system or the software/firmware doesn't apply to this system

Fixes

Corrected the temperature status of Seagate NVMe hard drives.

Online ROM Flash Component for VMware ESXi - Smart Array H240ar, H240nr, H240, H241, H244br, P240nr, P244br, P246br, P440ar, P440, P441, P542D, P741m, P840, P840ar, and P841
Version: 6.60 **(Recommended)**
Filename: CP035732.compsig; CP035732.zip

Fixes

- Issue where the QueryAsynchronousEvent could potentially provide incorrect response data
- Issue where the Cache could potentially get disable after several reboots

Enhancements

- Added support for larger SmartCache capacity size

Online ROM Flash Component for VMware ESXi - Smart Array P220i, P222, P420i, P420, P421, P721m, and P822
Version: 8.32 **(Recommended)**
Filename: CP033366.compsig; CP033366.zip

Fixes

System can potentially stop responding with no lockup code due to livelock condition where the RAID Stack thread is polling a queue for a completion to be returned by the base code firmware

Enhancements

Improved accuracy of drive temperature reporting feature

Online ROM Flash Component for VMware ESXi - Smart Array P230i, P430, P431, P731m, P830i, and P830
Version: 4.54 (B) **(Recommended)**
Filename: CP036098.compsig; CP036098.zip

Fixes

- DDR cache could be randomly disabled after several boots
- A hot-inserted replacement drive might show as a predictive failure if the original drive was identified as a predictive failure. Controller
- cache module might be marked as permanently disabled if the Smart Storage Battery is removed or failed while the system is online, even if SSA was previously used to enable write caching without a backup power source.
- Controller can become unresponsive due to a SmartCache pending flush operation when a read-ahead and a read-fill are performed in sequent.
- System might stop responding if a parity error is found during surface scan of a RAID6 volume. (POST Lockup 0x13)
- System fans might go to 100% if connected drives were spun down
- Issue where a controller crash dump may not be collected after a controller failure

---

Online ROM Flash Component for Windows (x64) - HPE 12Gb/s SAS Expander Firmware for HPE Smart Array Controllers and HPE HBA Controllers
Version: 4.02 (B) **(Optional)**
Filename: cp034755.compsig; cp034755.exe; cp034755.md5

Important Note!

- Customers who already have firmware version 4.02 installed do not need to update to 4.02 (B).
- Power cycle / cold reboot is required if firmware is upgraded from version 1.31 or earlier.

Enhancements

Added HPE Digital Signature

Online ROM Flash Component for Windows (x64) - HPE Apollo 2000 Gen10 Backplane Expander Firmware
Version: 1.00 **(Optional)**
Filename: cp031634.compsig; cp031634.exe; cp031634.md5

Enhancements

Initial Release

Online ROM Flash Component for Windows (x64) - HPE Apollo 2000 System - SAS Expander
Version: 1.00 (D) **(Recommended)**
Filename: cp034756.exe; cp034756.md5

Important Note!

- Customers who already have previous firmware version 1.00 installed do not need to update to 1.00(D).

Enhancements

Added HPE Digital Signature

Online ROM Flash Component for Windows (x64) - HPE Apollo 4200 Gen9 Backplane Expander Firmware
Version: 1.50 **(Optional)**
Filename: cp035218.exe; cp035218.md5

Important Note!

- Power cycle / cold reboot is required if firmware is upgraded from version 1.03 or earlier.

Enhancements

- Enhanced debug capabilities

Online ROM Flash Component for Windows (x64) - HPE Apollo 45xx Gen10 Backplane Expander Firmware
Version: 1.56 **(Optional)**
Filename: cp034415.compsig; cp034415.exe; cp034415.md5

Enhancements

- Supports Drive Zoning

Online ROM Flash Component for Windows (x64) - HPE Apollo 45xx Gen9 Backplane Expander Firmware
Version: 2.08 (B) **(Optional)**
Filename: cp034911.exe; cp034911.md5

Important Note!

- Customers who already have firmware version 2.08 installed do not need to update to 2.08(B).
- Please un-plug and re-plug the power cord to the server for firmware upgrade from version 1.03 or earlier to take effect.

Enhancements

Added HPE Digital Signature

Online ROM Flash Component for Windows (x64) - HPE Express Bay Enablement Switch Card
Version: 1.78 (B) **(Optional)**
Filename: cp034796.exe; cp034796.md5

Important Note!

- Customers who already have firmware version 1.78 installed do not need to update to 1.78(B).
- Power cycle / cold reboot is required after installation for updates to take effect.

Prerequisites

- The "HP ProLiant iLO 3/4 Channel Interface Driver" must be installed and running before using this flash component. If the driver is not running you will receive the following error message:

"Setup is unable to load a setup DLL"

- The HP ProLiant iLO firmware version must be v2.20 or later. If the HP ProLiant iLO firmware is older than v2.20 you will receive the following error message:

  Check dependency failed.

  Current version: iLOx x.xx

  Minimum version required: iLO4 2.20

  The software will not be installed on this system because the required hardware is not present in the system or the software/firmware doesn't apply to this system.

Enhancements

Added HPE Digital Signature

Online ROM Flash Component for Windows (x64) - HPE Host Bus Adapters H221
Version: 15.10.10.00 (C) **(Optional)**
Filename: cp034832.exe; cp034832.md5

Important Note!

This driver component supports Gen9 servers only with H221 controllers and the controller does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

Enhancements

- Added HPE Digital Signature

Supported Devices and Features

This driver component supports Gen9 servers only with H221 controllers and the controller does not support connection to D2600, D2700, and D6000 Disk Enclosures with Gen9 servers.

Online ROM Flash Component for Windows (x64) - HPE SAS Expander Firmware for HPE D2500sb Storage Blade
Version: 2.00 **(Optional)**
Filename: cp036364.compsig; cp036364.exe; cp036364.md5

Enhancements

Initial Release

Online ROM Flash Component for Windows (x64) - HPE Smart Array P408i-p, P408e-p, P408i-a, P408i-c, E208i-p, E208e-p, E208i-c, E208i-a, P408e-m, P204i-c, P204i-b, P816i-a and P416ie-m SR Gen10
Version: 1.34 (B) **(Recommended)**
Filename: cp036185.compsig; cp036185.exe; cp036185.md5

Important Note!

Note: If version 1.34 was previously installed, then it is not necessary to upgrade to version 1.34 (B).

Enhancements

- Added support for the HPE Smart Array P408e-m Controller.

Online ROM Flash Component for Windows (x64) - HPE Smart Array P824i-p MR Gen10
Version: 24.23.0-0019 (B) **(Optional)**
Filename: cp035040.compsig; cp035040.exe; cp035040.md5

Important Note!

- Customers who already have firmware version 24.23.0-0019 installed do not need to update to 24.23.0-0019(B).

Enhancements

- Added HPE Digital Signature

Online ROM Flash Component for Windows (x64) - Smart Array H240ar, H240nr, H240, H241, H244br, P240nr, P244br, P246br, P440ar, P440, P441,

P542D, P741m, P840, P840ar, and P841
Version: 6.60 **(Recommended)**
Filename: cp035731.exe; cp035731.md5

Fixes

- Issue where the QueryAsynchronousEvent could potentially provide incorrect response data
- Issue where the Cache could potentially get disable after several reboots

Enhancements

- Added support for larger SmartCache capacity size

Online ROM Flash Component for Windows (x64) - Smart Array P220i, P222, P420i, P420, P421, P721m, and P822
Version: 8.32 (B) **(Recommended)**
Filename: cp034910.exe; cp034910.md5

Important Note!

- Customers who already have firmware version 8.32 installed do not need to update to 8.32(B).

Enhancements

Added HPE Digital Signature

Online ROM Flash Component for Windows (x64) - Smart Array P230i, P430, P431, P731m, P830i, and P830
Version: 4.54 **(Optional)**
Filename: cp034040.exe; cp034040.md5

Fixes

- DDR cache could be randomly disabled after several boots
- A hot-inserted replacement drive might show as a predictive failure if the original drive was identified as a predictive failure. Controller
- cache module might be marked as permanently disabled if the Smart Storage Battery is removed or failed while the system is online, even if SSA was previously used to enable write caching without a backup power source.
- Controller can become unresponsive due to a SmartCache pending flush operation when a read-ahead and a read-fill are performed in sequent.
- System might stop responding if a parity error is found during surface scan of a RAID6 volume. (POST Lockup 0x13)
- System fans might go to 100% if connected drives were spun down
- Issue where a controller crash dump may not be collected after a controller failure

---

Supplemental Update / Online ROM Flash Component for Linux (x64) – HPE 12Gb/s SAS Expander Firmware for HPE Smart Array Controllers and HPE HBA Controllers
Version: 4.02 **(Optional)**
Filename: rpm/RPMS/x86_64/firmware-smartarray-2de15b6882-4.02-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-smartarray-2de15b6882-4.02-1.1.x86_64.rpm

Important Note!

- Power cycle / cold reboot is required if firmware is upgraded from version 1.31 or earlier.

Fixes

- Changed the Enclosure's Target and LUN address to the appropriate unique values. Previously these addresses would conflict with the SATA drive in bay #1 which interfered with software defined storage solutions such as Storage Spaces Direct.

Supplemental Update / Online ROM Flash Component for Linux (x64) - HPE Apollo 45xx Gen10 Backplane Expander Firmware
Version: 1.56 **(Optional)**
Filename: rpm/RPMS/x86_64/firmware-smartarray-815b1ae26d-1.56-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-smartarray-815b1ae26d-1.56-1.1.x86_64.rpm

Enhancements

- Supports Drive Zoning

Supplemental Update / Online ROM Flash Component for Linux (x64) – HPE Apollo 45xx Gen9 Backplane Expander Firmware
Version: 2.08 **(Optional)**
Filename: rpm/RPMS/x86_64/firmware-smartarray-7bdfcd246b-2.08-1.1.x86_64.rpm

Important Note!

- Please un-plug and re-plug the power cord to the server for firmware upgrade from version 1.03 or earlier to take effect.

Enhancements

- Enhanced debug capabilities.
- Improved integration with Smart Update Manager.

Supplemental Update / Online ROM Flash Component for Linux (x64) – HPE Express Bay Enablement Switch Card
Version: 1.78 **(Optional)**
Filename: firmware-smartarray-94189dca85-1.78-1.1.x86_64.rpm

Important Note!

- Power cycle / cold reboot is required after installation for updates to take effect.

Prerequisites

- Previous releases of HPE Express Bay Enablement Switch Card firmware Smart Component documented dependency on iLO 3/4 Channel Interface Driver. This driver is now included with the following Linux OSes:

  Red Hat Enterprise Linux 7 Server

  Red Hat Enterprise Linux 6 Server (x86-64)

  SUSE Linux Enterprise Server 12

- The HP ProLiant iLO firmware version must be v2.20 or later. If the HP ProLiant iLO firmware is older than v2.20 you will receive the following error message:

  Check dependency failed.

  Current version: iLOx x.xx

  Minimum version required: iLO4 2.20

  The software will not be installed on this system because the required hardware is not present in the system or the software/firmware doesn't apply to this system.

Fixes

- Corrected the temperature status of Seagate NVMe hard drives.

Supplemental Update / Online ROM Flash Component for Linux (x64) - HPE Smart Array P408i-p, P408e-p, P408i-a, P408i-c, E208i-p, E208e-p, E208i-c, E208i-a, P408e-m, P204i-c, P204i-b, P816i-a and P416ie-m SR Gen10
Version: 1.34 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-smartarray-f7c07bdbbd-1.34-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-smartarray-f7c07bdbbd-1.34-2.1.x86_64.rpm

Important Note!

Note: If version 1.34 was previously installed, then it is not necessary to upgrade to version 1.34 (B).

Enhancements

- Added support for the HPE Smart Array P408e-m Controller.

Supplemental Update / Online ROM Flash Component for Linux (x64) - Smart Array H240ar, H240nr, H240, H241, H244br, P240nr, P244br, P246br, P440ar, P440, P441, P542D, P741m, P840, P840ar, and P841
Version: 6.60 **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-smartarray-ea3138d8e8-6.60-1.1.x86_64.rpm

Important Note!

- In order to be detected properly, some controllers may need a newer version of the Smart Array driver installed prior to upgrading the controller firmware. If not installed, the component will fail with return code 3.
- When booting a system running Red Hat Enterprise Linux 7.1 Operating System, the HP Smart Array controllers might not be recognized. This issue is due to changes in the OS where the sg driver is no longer loaded during system boot. The work around for this issue is to manually issue a "**modprobe sg**" command which should load the sg driver. After the sg driver is loaded, the /dev/sg* devices should be present and the sg driver can be used to access SCSI devices.

Fixes

- Issue where the QueryAsynchronousEvent could potentially provide incorrect response data

- Issue where the Cache could potentially get disable after several reboots

Enhancements

- Added support for larger SmartCache capacity size

Supplemental Update / Online ROM Flash Component for Linux (x64) - Smart Array P220i, P222, P420i, P420, P421, P721m, and P822
Version: 8.32 **(Recommended)**
Filename: rpm/RPMS/x86_64/hp-firmware-smartarray-46a4d957a7-8.32-1.1.x86_64.rpm

Important Note!

- When booting a system running Red Hat Enterprise Linux 7.1 Operating System, the HP Smart Array controllers might not be recognized. This issue is due to changes in the OS where the sg driver is no longer loaded during system boot. The work around for this issue is to manually issue a "**modprobe sg**" command which should load the sg driver. After the sg driver is loaded, the /dev/sg* devices should be present and the sg driver can be used to access SCSI devices.

Fixes

System can potentially stop responding with no lockup code due to livelock condition where the RAID Stack thread is polling a queue for a completion to be returned by the base code firmware

Enhancements

Improved accuracy of drive temperature reporting feature

Supplemental Update / Online ROM Flash Component for Linux (x64) - Smart Array P230i, P430, P431, P731m, P830i, and P830
Version: 4.54 (B) **(Recommended)**
Filename: rpm/RPMS/x86_64/firmware-smartarray-112204add8-4.54-2.1.x86_64.rpm

Important Note!

- When booting a system running Red Hat Enterprise Linux 7.1 Operating System, the HP Smart Array controllers might not be recognized. This issue is due to changes in the OS where the sg driver is no longer loaded during system boot. The work around for this issue is to manually issue a "**modprobe sg**" command which should load the sg driver. After the sg driver is loaded, the /dev/sg* devices should be present and the sg driver can be used to access SCSI devices.

Fixes

- DDR cache could be randomly disabled after several boots
- A hot-inserted replacement drive might show as a predictive failure if the original drive was identified as a predictive failure. Controller
- cache module might be marked as permanently disabled if the Smart Storage Battery is removed or failed while the system is online, even if SSA was previously used to enable write caching without a backup power source.
- Controller can become unresponsive due to a SmartCache pending flush operation when a read-ahead and a read-fill are performed in sequent.
- System might stop responding if a parity error is found during surface scan of a RAID6 volume. (POST Lockup 0x13)
- System fans might go to 100% if connected drives were spun down
- Issue where a controller crash dump may not be collected after a controller failure

---

Firmware - Storage Fibre Channel Top

HPE Firmware Flash for Emulex Fibre Channel Host Bus Adapters for Linux (x64)
Version: 2018.06.01 **(Recommended)**
Filename: RPMS/x86_64/firmware-fc-emulex-2018.06.01-1.13.x86_64.compsig; RPMS/x86_64/firmware-fc-emulex-2018.06.01-1.13.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and

cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Firmware updates may be accomplished using the inbox or Out of Box (OOB) drivers. Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied enablement kit must be installed prior to this firmware component being identified by SUM for deployment.

The OOB driver and enablement kit are available on the Service Pack for ProLiant (SPP) which is available at http://www.hpe.com/servers/spp/download.

The Enablement Kit requires that the target environment have the libHBAAPI package installed from your OS installation media.

Install the FC Driver Kit, reboot, and then install the Enablement Kit.

Additional requirements:

Environment must be running the syslog daemon for the flash engine to run
Environment must have 32-bit netlink library (libnl.so) installed for component to be able to discover Emulex Host Bus Adapters(HBAs)

Enhancements

We have separate components to update fibre channel and converged network adapters. This is a fibre channel update component.

Added support to the following:

8G Standup and Mezzanine:

BIOS:

- Fabric assigned Boot Target/Logical Unit (LUN) to Fabric Assgined World Wide Name(FAWWN)

Updated 16/32 Gb HBA/Mezz universal boot
Updated 16Gb HBA/Mezz universal boot
Updated 8Gb HBA/Mezz universal boot

Contains:

16/32 Gb HBA/Mezz universal boot 11.4.334.10
16 Gb HBA/Mezz universal boot 11.4.334.11

8 Gb standup/mezz firmware 2.10X6

8 Gb standup/mezz universal boot image 11.40a13 (11.4.305.0 BIOS, 11.4.344.0 UEFI)

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

HPE Firmware Flash for Emulex Fibre Channel Host Bus Adapters for VMware vSphere 6.5
Version: 2018.06.01 **(Recommended)**
Filename: CP034217.compsig; CP034217.zip

Important Note!

Release Notes:

HPE StoreFabric Emulex Adapter Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Enhancements

We have separate components to update fibre channel and converged network adapters. This is a fibre channel update component.

Added support to the following:

8G Standup and Mezzanine:

BIOS:

- Fabric assigned Boot Target/Logical Unit (LUN) to Fabric Assgined World Wide Name(FAWWN)

Updated 16/32 Gb HBA/Mezz universal boot
Updated 16Gb HBA/Mezz universal boot
Updated 8Gb HBA/Mezz universal boot

Contains:

16/32 Gb HBA/Mezz universal boot 11.4.334.10
16 Gb HBA/Mezz universal boot 11.4.334.11

8 Gb standup/mezz firmware 2.10X6

8 Gb standup/mezz universal boot image 11.40a13 (11.4.305.0 BIOS, 11.4.344.0 UEFI)

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

Version: 2018.06.01 **(Recommended)**
Filename: CP034216.compsig; CP034216.zip

Important Note!

Release Notes:

HPE StoreFabric Emulex Adapter Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Enhancements

We have separate components to update fibre channel and converged network adapters. This is a fibre channel update component.

Added support to the following:

8G Standup and Mezzanine:

BIOS:

- Fabric assigned Boot Target/Logical Unit (LUN) to Fabric Assgined World Wide Name(FAWWN)

Updated 16/32 Gb HBA/Mezz universal boot
Updated 16Gb HBA/Mezz universal boot
Updated 8Gb HBA/Mezz universal boot

Contains:

16/32 Gb HBA/Mezz universal boot 11.4.334.10
16 Gb HBA/Mezz universal boot 11.4.334.11

8 Gb standup/mezz firmware 2.10x6

8 Gb standup/mezz universal boot image 11.40a13 (11.4.305.0 BIOS, 11.4.344.0 UEFI)

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

HPE Firmware Flash for Emulex Fibre Channel Host Bus Adapters for Windows 2012/2012 R2/2016 x64
Version: 2018.06.01 **(Recommended)**
Filename: cp034219.compsig; cp034219.exe

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied Emulex driver must be installed prior to this firmware component being identified by SUM for deployment. The OOB driver is available on the Service Pack for ProLiant (SPP) which is available at http://www.hpe.com/servers/spp/download/

Enhancements

We have separate components to update fibre channel and converged network adapters. This is a fibre channel update component.

Added support to the following:

8G Standup and Mezzanine:

BIOS:

- Fabric assigned Boot Target/Logical Unit (LUN) to Fabric Assgined World Wide Name(FAWWN)

Updated 16/32 Gb HBA/Mezz universal boot
Updated 16Gb HBA/Mezz universal boot
Updated 8Gb HBA/Mezz universal boot

Contains:

16/32 Gb HBA/Mezz universal boot 11.4.334.10
16 Gb HBA/Mezz universal boot 11.4.334.11

8 Gb standup/mezz firmware 2.10X6

8 Gb standup/mezz universal boot image 11.40a13 (11.4.305.0 BIOS, 11.4.344.0 UEFI)

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

HPE Firmware Flash for QLogic Fibre Channel Host Bus Adapters - Linux (x86_64)
Version: 2018.06.01 **(Recommended)**
Filename: RPMS/x86_64/firmware-fc-qlogic-2018.06.01-1.9.x86_64.compsig; RPMS/x86_64/firmware-fc-qlogic-2018.06.01-1.9.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric QLogic Adapter Release Notes

Prerequisites

Firmware updates may be accomplished using the inbox or Out of Box (OOB) drivers. Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied enablement kit must be installed prior to this firmware component being identified by SUM for deployment.

The OOB driver and enablement kit are available on the Service Pack for ProLiant (SPP) which is available at http://www.hpe.com/servers/spp/download.

Fixes

Fixed the following

8Gb Standup & 8Gb Mezzanine

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  Legacy BIOS (Basic Input Output System) Selectable Boot

16Gb Standup & 16Gb Mezzanine

Firmware

- Bring up up-link in 32G or 16G optical environment (FEC (Forward Error Correction) only) when connected with remote device that is not setting the SN bit to zero and TC bit to 1 at the same time during the speed negotiation phase and delays transmitting NOS during LQT phase.
- Dropped FCP_CMD frame by a virtual port (VP index greater than 0) logged into the fabric via Fabric Login (FLOGI) while the primary adapter port (VP0) was disabled via Global VP (Virtual Port) Options bit 2 of Initialize Multi-ID Firmware MBC (0048h).

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  Fabric Assigned WWPN (World Wide Port Name), Fabric Assigned Boot Logical Unit (LUN), Legacy BIOS (Basic Input Output System) Selectable Boot.

16Gb/32Gb Standup

Firmware

- Bring up up-link in 32G or 16G optical environment (FEC (Forward Error Correction) only) when connected with remote device that is not setting the SN bit to zero and TC bit to 1 at the same time during the speed negotiation phase and delays transmitting NOS during LQT phase.

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  FC (Fibre Channel) Tape, Fabric Assigned WWPN (World Wide Port Name), Fabric Assigned Boot LUN (Logical Unit), Legacy BIOS (Basic Input Output System) Selectable Boot.
- Changed Legacy BIOS (Basic Input Output System) Selectable Boot HII (Human Interface Infrastructure) default to Enabled.

Enhancements

Added support for the following:

16Gb Standup & 16Gb Mezzanine

- Power Loss calculation in D_port (Destination port) operation.

16Gb/32Gb Standup

- Power Loss calculation in D_port (Destination port) operation.
- Support maximum training timeout for 32Gbps data rate per FC-FS-4 (Fibre Channel Framing and Signaling) specification.

Updated the Firmware/BIOS/UEFI packages for 8 Gb, 16 Gb and 32 Gb products.

- 8 Gb HBA/Mezz
  - Package 3.77.08
  - Firmware 8.07.00
  - UEFI 6.64
  - BIOS 3.56
- 16 Gb HBA/Mezz
  - Package 6.01.59
  - Firmware 8.07.16
  - UEFI 6.63
  - BIOS 3.43
- 16/32 Gb
  - Package 01.70.85
  - Firmware 8.07.18
  - UEFI 6.47
  - BIOS 3.54

Supported Devices and Features

This firmware supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

HPE Firmware Flash for QLogic Fibre Channel Host Bus Adapters for VMware vSphere 6.0
Version: 2018.06.01 **(Recommended)**
Filename: CP034228.compsig; CP034228.zip

Important Note!

HPE StoreFabric QLogic Adapter Release Notes

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied Qlogic driver must be installed prior to this firmware component being identified by SUM for deployment. The OOB driver is available on the Service Pack for ProLiant (SPP) which is available at http://www.hpe.com/servers/spp/download/

Fixes

Fixed the following

8Gb Standup & 8Gb Mezzanine

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  Legacy BIOS (Basic Input Output System) Selectable Boot

16Gb Standup & 16Gb Mezzanine

Firmware

- Bring up up-link in 32G or 16G optical environment (FEC (Forward Error Correction) only) when connected with remote device that is not setting the SN bit to zero and TC bit to 1 at the same time during the speed negotiation phase and delays transmitting NOS during LQT phase.
- Dropped FCP_CMD frame by a virtual port (VP index greater than 0) logged into the fabric via Fabric Login (FLOGI) while the primary adapter port (VP0) was disabled via Global VP (Virtual Port) Options bit 2 of Initialize Multi-ID Firmware MBC (0048h).

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  Fabric Assigned WWPN (World Wide Port Name), Fabric Assigned Boot Logical Unit (LUN), Legacy BIOS (Basic Input Output System) Selectable Boot.

16Gb/32Gb Standup

Firmware

- Bring up up-link in 32G or 16G optical environment (FEC (Forward Error Correction) only) when connected with remote device that is not setting the SN bit to zero and TC bit to 1 at the same time during the speed negotiation phase and delays transmitting NOS during LQT phase.

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  FC (Fibre Channel) Tape, Fabric Assigned WWPN (World Wide Port Name), Fabric Assigned Boot LUN (Logical Unit), Legacy BIOS (Basic Input Output System) Selectable Boot.
- Changed Legacy BIOS (Basic Input Output System) Selectable Boot HII (Human Interface Infrastructure) default to Enabled.

Enhancements

Added support for the following:

16Gb Standup & 16Gb Mezzanine

- Power Loss calculation in D_port (Destination port) operation.

16Gb/32Gb Standup

- Power Loss calculation in D_port (Destination port) operation.
- Support maximum training timeout for 32Gbps data rate per FC-FS-4 (Fibre Channel Framing and Signaling) specification.

Updated the Firmware/BIOS/UEFI packages for 8 Gb, 16 Gb and 32 Gb products.

- 8 Gb HBA/Mezz
  - Package 3.77.08
  - Firmware 8.07.00
  - UEFI 6.64
  - BIOS 3.56
- 16 Gb HBA/Mezz
  - Package 6.01.59
  - Firmware 8.07.16
  - UEFI 6.63
  - BIOS 3.43
- 16/32 Gb
  - Package 01.70.85
  - Firmware 8.07.18
  - UEFI 6.47
  - BIOS 3.54

Supported Devices and Features

This firmware supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

HPE Firmware Flash for QLogic Fibre Channel Host Bus Adapters for VMware vSphere 6.5
Version: 2018.06.01 **(Recommended)**
Filename: CP034229.compsig; CP034229.zip

Important Note!

HPE StoreFabric QLogic Adapter Release Notes

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied Qlogic driver must be installed prior to this firmware component being identified by SUM for deployment. The OOB driver is available on the Service Pack for ProLiant (SPP) which is available at http://www.hpe.com/servers/spp/download/

Fixes

Fixed the following

8Gb Standup & 8Gb Mezzanine

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  Legacy BIOS (Basic Input Output System) Selectable Boot

16Gb Standup & 16Gb Mezzanine

Firmware

- Bring up up-link in 32G or 16G optical environment (FEC (Forward Error Correction) only) when connected with remote device that is not setting the SN bit to zero and TC bit to 1 at the same time during the speed negotiation phase and delays transmitting NOS during LQT phase.
- Dropped FCP_CMD frame by a virtual port (VP index greater than 0) logged into the fabric via Fabric Login (FLOGI) while the primary adapter port (VP0) was disabled via Global VP (Virtual Port) Options bit 2 of Initialize Multi-ID Firmware MBC (0048h).

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  Fabric Assigned WWPN (World Wide Port Name), Fabric Assigned Boot Logical Unit (LUN), Legacy BIOS (Basic Input Output System) Selectable Boot.

16Gb/32Gb Standup

Firmware

- Bring up up-link in 32G or 16G optical environment (FEC (Forward Error Correction) only) when connected with remote device that is not setting the SN bit to zero and TC bit to 1 at the same time during the speed negotiation phase and delays transmitting NOS during

LQT phase.

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  FC (Fibre Channel) Tape, Fabric Assigned WWPN (World Wide Port Name), Fabric Assigned Boot LUN (Logical Unit), Legacy BIOS (Basic Input Output System) Selectable Boot.
- Changed Legacy BIOS (Basic Input Output System) Selectable Boot HII (Human Interface Infrastructure) default to Enabled.

Enhancements

Added support for the following:

16Gb Standup & 16Gb Mezzanine

- Power Loss calculation in D_port (Destination port) operation.

16Gb/32Gb Standup

- Power Loss calculation in D_port (Destination port) operation.
- Support maximum training timeout for 32Gbps data rate per FC-FS-4 (Fibre Channel Framing and Signaling) specification.

Updated the Firmware/BIOS/UEFI packages for 8 Gb, 16 Gb and 32 Gb products.

- 8 Gb HBA/Mezz
  - Package 3.77.08
  - Firmware 8.07.00
  - UEFI 6.64
  - BIOS 3.56
- 16 Gb HBA/Mezz
  - Package 6.01.59
  - Firmware 8.07.16
  - UEFI 6.63
  - BIOS 3.43
- 16/32 Gb
  - Package 01.70.85
  - Firmware 8.07.18
  - UEFI 6.47
  - BIOS 3.54

Supported Devices and Features

This firmware supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

HPE Firmware Online Flash for QLogic Fibre Channel Host Bus Adapters - Windows 2012/2012R2/2016 (x86_64)
Version: 2018.06.01 **(Recommended)**
Filename: cp034231.compsig; cp034231.exe

Important Note!

Release Notes:
HPE StoreFabric QLogic Adapters Release Notes

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The OOB driver is available on the Service Pack for ProLiant (SPP) which is available at http://www.hpe.com/servers/spp/download.

Fixes

Fixed the following

8Gb Standup & 8Gb Mezzanine

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  Legacy BIOS (Basic Input Output System) Selectable Boot

16Gb Standup & 16Gb Mezzanine

Firmware

- Bring up up-link in 32G or 16G optical environment (FEC (Forward Error Correction) only) when connected with remote device that is not setting the SN bit to zero and TC bit to 1 at the same time during the speed negotiation phase and delays transmitting NOS during LQT phase.
- Dropped FCP_CMD frame by a virtual port (VP index greater than 0) logged into the fabric via Fabric Login (FLOGI) while the primary adapter port (VP0) was disabled via Global VP (Virtual Port) Options bit 2 of Initialize Multi-ID Firmware MBC (0048h).

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  Fabric Assigned WWPN (World Wide Port Name), Fabric Assigned Boot Logical Unit (LUN), Legacy BIOS (Basic Input Output System) Selectable Boot.

16Gb/32Gb Standup

Firmware

- Bring up up-link in 32G or 16G optical environment (FEC (Forward Error Correction) only) when connected with remote device that is not setting the SN bit to zero and TC bit to 1 at the same time during the speed negotiation phase and delays transmitting NOS during LQT phase.

UEFI

- Firmware Management Protocol now supports flashing older Multiboot versions.
- Firmware Management Protocol SetImage no longer displays dots on the screen.
- The following HII (Human Interface Infrastructure) fields now require a reboot after value change:
  FC (Fibre Channel) Tape, Fabric Assigned WWPN (World Wide Port Name), Fabric Assigned Boot LUN (Logical Unit), Legacy BIOS (Basic Input Output System) Selectable Boot.
- Changed Legacy BIOS (Basic Input Output System) Selectable Boot HII (Human Interface Infrastructure) default to Enabled.

Enhancements

Added support for the following:

16Gb Standup & 16Gb Mezzanine

- Power Loss calculation in D_port (Destination port) operation.

16Gb/32Gb Standup

- Power Loss calculation in D_port (Destination port) operation.
- Support maximum training timeout for 32Gbps data rate per FC-FS-4 (Fibre Channel Framing and Signaling) specification.

Updated the Firmware/BIOS/UEFI packages for 8 Gb, 16 Gb and 32 Gb products.

- 8 Gb HBA/Mezz
  - Package 3.77.08
  - Firmware 8.07.00
  - UEFI 6.64
  - BIOS 3.56
- 16 Gb HBA/Mezz
  - Package 6.01.59
  - Firmware 8.07.16
  - UEFI 6.63

        - BIOS 3.43

    - 16/32 Gb
        - Package 01.70.85
        - Firmware 8.07.18
        - UEFI 6.47
        - BIOS 3.54

Supported Devices and Features

This firmware supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

Firmware - System Top

Online Flash Component for Linux - Gen10 NVMe Backplane PIC Firmware
Version: 1.20 (D) **(Optional)**
Filename: RPMS/x86_64/firmware-nvmebackplane-gen10-1.20-4.1.x86_64.compsig; RPMS/x86_64/firmware-nvmebackplane-gen10-1.20-4.1.x86_64.rpm

Important Note!

Note: After running this component to update the NVMe Backplane PIC firmware, a server reboot is required for iLO to display the new NVMe Backplane PIC firmware version on iLO's Firmware Information page

Prerequisites

iLO 5 version 1.10 or later is required.

Fixes

Firmware Package version 1.20(D) addressed the following issue:

- When using OneView, attempts to upgrade firmware from version 1.18 to 1.20 failed.

Note: If the target device was previously updated to firmware version 1.20, it is not necessary to apply firmware update 1.20(D).

Enhancements

The following support was added in version 1.20(C). No new features were added in version 1.20(D).

- Added support for the HPE ProLiant XL270d Gen10 Server

Online Flash Component for Linux - NVMe Backplane PIC Firmware
Version: 8.4 (C) **(Optional)**
Filename: RPMS/i386/firmware-nvmebackplane-8.4-3.1.i386.rpm

Prerequisites

iLO 4 version 2.50 or later is required.

Enhancements

- Updated to support Service Pack for ProLiant version 2017.07.0

Note: If version 8.4 was previously installed, then it is not necessary to upgrade to version 8.4 (C).

Online Flash Component for VMware - NVMe Backplane PIC Firmware
Version: 8.4 (C) **(Optional)**
Filename: CP033323.compsig; CP033323.zip

Prerequisites

iLO 4 version 2.50 or later is required.

Enhancements

- Updated to support Service Pack for ProLiant version 2017.07.0

  Note: If version 8.4 was previously installed, then it is not necessary to upgrade to version 8.4 (C).

Online Flash Component for Windows x64 - Gen10 NVMe Backplane PIC Firmware
Version: 1.20 (C) **(Optional)**
Filename: cp036570.compsig; cp036570.exe

Important Note!

Note: After running this component to update the NVMe Backplane PIC firmware, a server reboot is required for iLO to display the new NVMe Backplane PIC firmware version on iLO's Firmware Information page

Prerequisites

iLO 5 version 1.10 or later is required.

Fixes

Firmware Package version 1.20(C) addressed the following issue:

- When using OneView, attempts to upgrade firmware from version 1.18 to 1.20 failed.

Note: If the target device was previously updated to firmware version 1.20, it is not necessary to apply firmware update 1.20(C).

Enhancements

The following support was added in version 1.20(B). No new features were added in version 1.20(C).

- Added support for the HPE ProLiant XL270d Gen10 Server

Online Flash Component for Windows x64 - NVMe Backplane PIC Firmware
Version: 8.4 (D) **(Optional)**
Filename: cp034942.exe

Prerequisites

iLO 4 version 2.50 or later is required.

Fixes

- Resolved an information disclosure vulnerability issue; ref: CVE-2017-8992

  Note: If version 8.4 was previously installed, then it is not necessary to upgrade to version 8.4 (D).

Firmware (Entitlement Required) - Storage Controller Top

HP D6000 6Gb SAS Disk Enclosure ROM Flash Component for Windows (x64)
Version: 2.98 **(Critical)**
Filename: cp029908.exe; cp029908.md5

Important Note!

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

IMPORTANT: Power up/down sequence is important to maintain integrity of the configuration, please refer to "HP D6000 Disk Enclosure User Guide" document for more details.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to %systemdrive%\CPQSYSTEM\Log\Verbose.log and flash summary is logged to %systemdrive%\CPQSYSTEM\Log\cpqsetup.log.

Prerequisites

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE:All firmware flash progress messages are logged to %systemdrive%\CPQSYSTEM\Log\Verbose.log and flash summary is logged to %systemdrive%\CPQSYSTEM\Log\cpqsetup.log.

Fixes

Following issue is fixed in this version of firmware:

Changed the settings in the SAS Expander to support disk discovery when 12Gb SAS HDDs are installed in the enclosure

Supported Devices and Features

HP D6000 Disk Enclosure can be connected behind any of the following devices :

- HP H222 Host Bus Adapter
- HP H221 Host Bus Adapter
- HP H241 Smart Host Bus Adapter
- HP Smart Array P731m Controller
- HP Smart Array P741m Controller
- HP Smart Array P721m Controller
- HP Smart Array P441 Controller
- HP Smart Array P431 Controller
- HP Smart Array P822 Controller
- HP Smart Array P841 Controller
- HP Smart Array P421 Controller

HP D2600/D2700 6Gb SAS Disk Enclosure ROM Flash Component for Linux (x64)
Version: 0150 (B) **(Recommended)**
Filename: RPMS/x86_64/hp-firmware-d2600-d2700-0150-2.1.x86_64.rpm

Important Note!

Firmware upgrade to 150(B) is not necessary, if the device is currently running 150 firmware

IMPORTANT:Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: When disk enclosures are cascaded, I/O module A of one enclosure is connected to I/O module A of the subsequent enclosure. During a firmware update, I/O module A in the cascaded disk enclosures is automatically updated.

In dual-domain configurations, both I/O modules of the target disk enclosure and cascaded disk enclosures are automatically updated during the firmware installation process.

All firmware flash progress messages are logged to /var/cpq/Component.log .

Prerequisites

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: When disk enclosures are cascaded, I/O module A of one enclosure is connected to I/O module A of the subsequent enclosure. During a firmware update, I/O module A in the cascaded disk enclosures is automatically updated.

In dual-domain configurations, both I/O modules of the target disk enclosure and cascaded disk enclosures are automatically updated during the firmware installation process.

All firmware flash progress messages are logged to /var/cpq/Component.log.

Fixes

The following fix is added in this version:-

-Removed action over FAULT_SENSED bit due to incorrect algorithm.

Supported Devices and Features

The D2600/ D2700 Enclosure can be attached to any of the following HP Storage Controllers and Host Bus Adapters:

HP H222 Host Bus Adapter
HP H221 Host Bus Adapter
HP H241 Smart Host Bus Adapter
HP Smart Array P812 Controller
HP Smart Array P822 Controller
HP Smart Array P841 Controller
HP Smart Array P441 Controller
HP Smart Array P431 Controller
HP Smart Array P421 Controller
HP Smart Array P411 Controller
HP Smart Array P212 Controller
HP Smart Array P222 Controller

HP D2600/D2700 6Gb SAS Disk Enclosure ROM Flash Component for Windows (x64)
Version: 0150 (B) **(Recommended)**
Filename: cp028806.exe

Important Note!

Firmware upgrade to 150(B) is not necessary, if the device is currently running 150 firmware

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: When disk enclosures are cascaded, I/O module A of one enclosure is connected to I/O module A of the subsequent enclosure. During a firmware update, I/O module A in the cascaded disk enclosures is automatically updated.

In dual-domain configurations, both I/O modules of the target disk enclosure and cascaded disk enclosures are automatically updated during the firmware installation process.

All firmware flash progress messages are logged to %systemdrive%\CPQSYSTEM\Log\D2000.log and flash summary is logged to %systemdrive%\CPQSYSTEM\Log\cpqsetup.log.

Prerequisites

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: When disk enclosures are cascaded, I/O module A of one enclosure is connected to I/O module A of the subsequent enclosure. During a firmware update, I/O module A in the cascaded disk enclosures is automatically updated.

In dual-domain configurations, both I/O modules of the target disk enclosure and cascaded disk enclosures are automatically updated during the firmware installation process.

All firmware flash progress messages are logged to %systemdrive%\CPQSYSTEM\Log\D2000.log and flash summary is logged to %systemdrive%\CPQSYSTEM\Log\cpqsetup.log.

Fixes

The following fix is added in this version:-

-Removed action over FAULT_SENSED bit due to incorrect algorithm.

Supported Devices and Features

The D2600/ D2700 Enclosure can be attached to any of the following HP Storage Controllers and Host Bus Adapters:

HP H222 Host Bus Adapter
HP H221 Host Bus Adapter
HP H241 Smart Host Bus Adapter
HP Smart Array P812 Controller
HP Smart Array P822 Controller
HP Smart Array P841 Controller
HP Smart Array P441 Controller
HP Smart Array P431 Controller
HP Smart Array P421 Controller
HP Smart Array P411 Controller
HP Smart Array P212 Controller
HP Smart Array P222 Controller

HP D6000 6Gb SAS Disk Enclosure ROM Flash Component for Linux (x64)
Version: 2.98 **(Critical)**
Filename: RPMS/x86_64/hp-firmware-smartarray-d6000-2.98-1.1.x86_64.rpm

Important Note!

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

IMPORTANT: Power up/down sequence is important to maintain integrity of the configuration, please refer to "HP D6000 Disk Enclosure User Guide" document for more details.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/Verbose.log and flash summary is logged to /var/cpq/Component.log.

Prerequisites

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE:All firmware flash progress messages are logged to /var/cpq/Verbose.log and flash summary is logged to /var/cpq/Component.log.

Fixes

Following issue is fixed in this version of firmware:

Changed the settings in the SAS Expander to support disk discovery when 12Gb SAS HDDs are installed in the enclosure

Supported Devices and Features

HP D6000 Disk Enclosure can be connected behind any of the following devices :

- HP H222 Host Bus Adapter
- HP H221 Host Bus Adapter
- HP H241 Smart Host Bus Adapter
- HP Smart Array P731m Controller
- HP Smart Array P741m Controller
- HP Smart Array P721m Controller
- HP Smart Array P441 Controller
- HP Smart Array P431 Controller
- HP Smart Array P822 Controller
- HP Smart Array P841 Controller
- HP Smart Array P421 Controller

HP D6000 6Gb SAS Disk Enclosure ROM Flash Component for VMware (esxi)
Version: 2.98 **(Critical)**
Filename: CP029051.md5; CP029051.zip

Important Note!

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

IMPORTANT: Power up/down sequence is important to maintain integrity of the configuration, please refer to HP D6000 Disk Enclosure User Guide document for more details.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/Verbose.log and flash summary is logged to /var/cpq/Component.log.

Prerequisites

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE:All firmware flash progress messages are logged to /var/cpq/Verbose.log and flash summary is logged to /var/cpq/Component.log.

Fixes

Following issue is fixed in this version of firmware:

Changed the settings in the SAS Expander to support disk discovery when 12Gb SAS HDDs are installed in the enclosure

Supported Devices and Features

HP D6000 Disk Enclosure can be connected behind any of the following devices :

- HP H222 Host Bus Adapter
- HP H221 Host Bus Adapter
- HP H241 Smart Host Bus Adapter
- HP Smart Array P731m Controller
- HP Smart Array P741m Controller
- HP Smart Array P721m Controller
- HP Smart Array P441 Controller
- HP Smart Array P431 Controller
- HP Smart Array P822 Controller
- HP Smart Array P841 Controller
- HP Smart Array P421 Controller

HPE D3600/D3700/D3610/D3710 12Gb SAS Disk Enclosure ROM Flash Component for Linux (x64)
Version: 4.04 (A) **(Recommended)**
Filename: CP034654.md5; RPMS/x86_64/firmware-d3000-4.04-1.1.x86_64.compsig; RPMS/x86_64/firmware-d3000-4.04-1.1.x86_64.rpm

Important Note!

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted. In single domain configuration, if user hosts an OS in D3000(or any storage box) and flash the SEPs, it will hang/crash everytime as SmartComponent will reset the SEPs after flash/codeload.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/D3000.log and flash summary is logged to /var/cpq/Component.log.

Prerequisites

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/D3000.log and flash summary is logged to /var/cpq/Component.log.

Fixes

The following fix was incorporated in this version:

- Fixed NVRAM CRC error

Please refer to the Release Notes for the complete listing of fixes, enhancements, known issues and work-arounds corresponding to this firmware.

Supported Devices and Features

The D3600 / D3700 / D3610 / D3710 Enclosure can be attached to any of the following HPE Storage Controllers and Host Bus Adapters :

- HP Smart Array P841 Controller
- HP Smart Array P441 Controller
- HP Smart HBA H241
- HPE Smart Array P408e-p Controller
- HPE Smart Array E208e-p Controller
- HPE Smart Array P408e-m Controller
- HP Smart Array P741m Controller

HPE D3600/D3700/D3610/D3710 12Gb SAS Disk Enclosure ROM Flash Component for VMware (ESXi)
Version: 4.04 (A) **(Recommended)**
Filename: CP034653.compsig; CP034653.md5; CP034653.zip

Important Note!

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted. In single domain configuration, if user hosts an OS in D3000(or any storage box) and flash the SEPs, it will hang/crash everytime as SmartComponent will reset the SEPs after flash/codeload.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/D3000.log and flash summary is logged to /var/cpq/Component.log.

Prerequisites

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/D3000.log and flash summary is logged to /var/cpq/Component.log.

Fixes

The following fix was incorporated in this version:

- Fixed NVRAM CRC error

Please refer to the Release Notes for the complete listing of fixes, enhancements, known issues and work-arounds corresponding to this firmware.

Supported Devices and Features

The D3600 / D3700 / D3610 / D3710 Enclosure can be attached to any of the following HPE Storage Controllers and Host Bus Adapters :

- HP Smart Array P841 Controller
- HP Smart Array P441 Controller
- HP Smart HBA H241
- HP Smart Array P741m Controller

HPE D3600/D3700/D3610/D3710 12Gb SAS Disk Enclosure ROM Flash Component for Windows (x64)
Version: 4.04 (A) **(Recommended)**
Filename: cp034655.compsig; cp034655.exe

Important Note!

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted. In single domain configuration, if user hosts an OS in D3000(or any storage box) and flash the SEPs, it will hang/crash everytime as SmartComponent will reset the SEPs after flash/codeload.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to %systemdrive%\CPQSYSTEM\Log\D3000.log and flash summary is logged to %systemdrive%\CPQSYSTEM\Log\cpqsetup.log.

Prerequisites

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to %systemdrive%\CPQSYSTEM\Log\D3000.log and flash summary is logged to %systemdrive%\CPQSYSTEM\Log\cpqsetup.log.

Fixes

The following fix was incorporated in this version:

- Fixed NVRAM CRC error

Please refer to the Release Notes for the complete listing of fixes, enhancements, known issues and work-arounds corresponding to this firmware.

Supported Devices and Features

The D3600 / D3700 / D3610 / D3710 Enclosure can be attached to any of the following HPE Storage Controllers and Host Bus Adapters :

- HP Smart Array P841 Controller
- HP Smart Array P441 Controller
- HP Smart HBA H241
- HPE Smart Array P408e-p Controller
- HPE Smart Array E208e-p Controller
- HPE Smart Array P408e-m Controller

- HP Smart Array P741m Controller

HPE D6020 12Gb SAS Disk Enclosure ROM Flash Component for Linux (x64)
Version: 2.72 **(Recommended)**
Filename: CP035199.md5; RPMS/x86_64/firmware-d6020-2.72-1.1.x86_64.compsig; RPMS/x86_64/firmware-d6020-2.72-1.1.x86_64.rpm

Important Note!

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted. In single domain configuration, if user hosts an OS in D6020(or any storage box) and flash the SEPs, it will hang/crash everytime as SmartComponent will reset the SEPs after flash/codeload.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/D6020.log and flash summary is logged to /var/cpq/Component.log.

Prerequisites

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/D6020.log and flash summary is logged to /var/cpq/Component.log.

Fixes

The following fixes was incorporated in this version:

- Sensors presence reporting for single domain mode
- When an IOM is pulled the surviving IOM reports False critical temperatures
- Configure phy zone group to 0 (zero) for all phys in the initstring

Please refer to the Release Notes for the complete listing of fixes, enhancements, known issues and work-arounds corresponding to this firmware.

Supported Devices and Features

The D6020 Enclosure can be attached to any of the following HPE Storage Controllers and Host Bus Adapters :

- HP Smart Array P841 Controller
- HP Smart Array P441 Controller
- HP Smart HBA H241
- HPE Smart Array P408e-p Controller
- HPE Smart Array E208e-p Controller
- HPE Smart Array P408e-m Controller
- HP Smart Array P741m Controller

HPE D6020 12Gb SAS Disk Enclosure ROM Flash Component for VMware (ESXi)
Version: 2.72 **(Recommended)**
Filename: CP035198.compsig; CP035198.md5; CP035198.zip

Important Note!

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted. In single domain configuration, if user hosts an OS in D6020(or any storage box) and flash the SEPs, it will hang/crash everytime as SmartComponent will reset the SEPs after flash/codeload.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/D6020.log and flash summary is logged to /var/cpq/Component.log.

Prerequisites

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to /var/cpq/D6020.log and flash summary is logged to /var/cpq/Component.log.

Fixes

The following fixes was incorporated in this version:

- Sensors presence reporting for single domain mode
- When an IOM is pulled the surviving IOM reports False critical temperatures
- Configure phy zone group to 0 (zero) for all phys in the initstring

Please refer to the Release Notes for the complete listing of fixes, enhancements, known issues and work-arounds corresponding to this firmware.

Supported Devices and Features

The D6020 Enclosure can be attached to any of the following HPE Storage Controllers and Host Bus Adapters :

- HP Smart Array P841 Controller
- HP Smart Array P441 Controller
- HP Smart HBA H241
- HP Smart Array P741m Controller

HPE D6020 12Gb SAS Disk Enclosure ROM Flash Component for Windows (x64)
Version: 2.72 **(Recommended)**
Filename: cp035200.compsig; cp035200.exe

Important Note!

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted. In single domain configuration, if user hosts an OS in D6020(or any storage box) and flash the SEPs, it will hang/crash everytime as SmartComponent will reset the SEPs after flash/codeload.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to %systemdrive%\CPQSYSTEM\Log\D6020.log and flash summary is logged to %systemdrive%\CPQSYSTEM\Log\cpqsetup.log.

Prerequisites

IMPORTANT: Firmware updates must be performed during a system maintenance window, with all I/O to the system halted.

WARNING! Do not power cycle or restart during the firmware update as this can result in loss of capabilities for this unit. It typically takes several minutes for the firmware to load.

NOTE: All firmware flash progress messages are logged to %systemdrive%\CPQSYSTEM\Log\D6020.log and flash summary is logged to %systemdrive%\CPQSYSTEM\Log\cpqsetup.log.

Fixes

The following fixes was incorporated in this version:

- Sensors presence reporting for single domain mode
- When an IOM is pulled the surviving IOM reports False critical temperatures
- Configure phy zone group to 0 (zero) for all phys in the initstring

Please refer to the Release Notes for the complete listing of fixes, enhancements, known issues and work-arounds corresponding to this firmware.

Supported Devices and Features

The D6020 Enclosure can be attached to any of the following HPE Storage Controllers and Host Bus Adapters :

- HP Smart Array P841 Controller
- HP Smart Array P441 Controller
- HP Smart HBA H241
- HPE Smart Array P408e-p Controller
- HPE Smart Array E208e-p Controller
- HPE Smart Array P408e-m Controller
- HP Smart Array P741m Controller

Software - Lights-Out Management Top

HP Lights-Out Online Configuration Utility for Linux (AMD64/EM64T)
Version: 5.3.0-0 **(Optional)**
Filename: hponcfg-5.3.0-0.x86_64.compsig; hponcfg-5.3.0-0.x86_64.rpm

Prerequisites

This utility requires the following minimum firmware revisions:

- Integrated Lights-Out 3 firmware v1.00 or later
- Integrated Lights-Out 4 firmware v1.00 or later
- Integrated Lights-Out 5 firmware v1.20 or later

The management interface driver and management agents must be installed on the server.

For iLO 5, openssl v1.0.x or later is required in addition to above packages.
Customers who manually compile and install openssl or intentionally relocate /usr/bin/openssl, need to set PATH environment variable to direct HPONCFG to the right/intended openssl.

Enhancements

Introduced support for iLO 5 v1.30.

HP Lights-Out Online Configuration Utility for Windows x64 Editions
Version: 5.2.0.0 **(Recommended)**
Filename: cp033351.compsig; cp033351.exe

Important Note!

HPONCFG for Windows Server supports iLO in PRODUCTION/HIGH/FIPS security state only.

Prerequisites

This utility requires the following minimum firmware revisions:

- Integrated Lights-Out 3 firmware v1.00 or later
- Integrated Lights-Out 4 firmware v1.00 or later
- Integrated Lights-Out 5 firmware v1.10 or later

The management interface driver must be installed on the server.

Microsoft .Net Framework 2.0 or later is required to launch HPONCFG GUI.

Fixes

Fixed issue where IML and IEL logs were not cleared after doing iLO factory default.

Enhancements

Introduced support for iLO 5 v1.20 or later.

Software - Management Top

HPE SDK Python Module
Version: 2.0.0 **(Optional)**
Filename: python-ilorest-library-2.0.0.zip

Enhancements

Support for Gen10 Servers.

HPE SDK Python Module
Version: 2.3 **(Optional)**
Filename: python-ilorest-library-2.3.0.zip

Enhancements

- Added the ability to set functions to encode/decode sensitive cache data.
- Increased validation and load times.

HPE SDK Python RPM
Version: 1.3.0 **(Optional)**
Filename: decorator-3.4.0-1.noarch.rpm; decorator-3.4.0-1.src.rpm; jsonpatch-1.3-1.noarch.rpm; jsonpatch-1.3-1.src.rpm; jsonpath-rw-1.3.0-1.noarch.rpm; jsonpath-rw-1.3.0-1.src.rpm; jsonpointer-1.1-1.noarch.rpm; jsonpointer-1.1-1.src.rpm; ply-3.4-1.noarch.rpm; ply-3.4-1.src.rpm; python-ilorest-library-1.3.0-1.noarch.rpm; python-ilorest-library-1.3.0-1.src.rpm; recordtype-1.1-1.noarch.rpm; recordtype-1.1-1.src.rpm; six-1.7.2-1.noarch.rpm; six-1.7.2-1.src.rpm; urlparse2-1.1.1-1.noarch.rpm; urlparse2-1.1.1-1.src.rpm; validictory-1.0.1-1.noarch.rpm; validictory-1.0.1-1.src.rpm

Fixes

Initial version.

HPE SDK Python RPM
Version: 2.3.0 **(Optional)**
Filename: decorator-4.1.2-1.noarch.rpm; jsonpatch-1.16-1.noarch.rpm; jsonpath-rw-1.4.0-1.noarch.rpm; jsonpointer-1.10-1.noarch.rpm; ply-3.10-1.noarch.rpm; python-ilorest-library-2.3.0-1.noarch.rpm; recordtype-1.1-1.noarch.rpm; six-1.10.0-1.noarch.rpm; urlparse2-1.1.1-1.noarch.rpm; validictory-1.1.1-1.noarch.rpm

Enhancements

Latest rpm release

Management Bundle Smart Component for ESXi 6.0
Version: 2018.06.01 **(Recommended)**
Filename: cp034609.compsig; cp034609.zip
Driver Name and Version:

Fixes

WBEM Providers

- Fixed issue with Smart Array Provider reporting change of battery status frequently

Agentless Management Service

- Fixed to remove heartbeat trap (cpqHo2GenericTrap) delivery at OS boot when periodic test trap feature is disabled
- Fixed memory leak partly caused by AMS running in the OS init resource group
- Fixed reporting of the embedded SATA controller to resolve missing drives in the iLO Storage Tab display

Enhancements

WBEM Providers

- Added support for Smart Array Controller model P408i-sb

Agentless Management Service

- Added reporting of OS Logical Disk Volume Configuration and Utilization to iLO's Active Health System Log

---

Management Bundle Smart Component for ESXi 6.5
Version: 2018.06.01 **(Recommended)**
Filename: cp034610.compsig; cp034610.zip
Driver Name and Version:

Fixes

WBEM Providers

- Fixed issue with Smart Array Provider reporting change of battery status frequently

Agentless Management Service

- Fixed to remove heartbeat trap (cpqHo2GenericTrap) delivery at OS boot when periodic test trap feature is disabled
- Fixed memory leak partly caused by AMS running in the OS init resource group
- Fixed reporting of the embedded SATA controller to resolve missing drives in the iLO Storage Tab display

Enhancements

WBEM Providers

- Added support for Smart Array Controller model P408i-sb

Agentless Management Service

- Added reporting of OS Logical Disk Volume Configuration and Utilization to iLO's Active Health System Log

Software - Network Top

Broadcom Active Health System Agent for HPE ProLiant Network Adapters for Linux x86_64
Version: 1.0.20-1 (B) **(Optional)**
Filename: hp-tg3sd-1.0.20-1.x86_64.compsig; hp-tg3sd-1.0.20-1.x86_64.rpm; hp-tg3sd-1.0.20-1.x86_64.txt

Fixes

SUM no longer attempts to install this product on Gen10 servers, which this product does not support.

Supported Devices and Features

This software supports the following Broadcom network adapters:

- HP Ethernet 1Gb 2-port 330i Adapter (22BD)
- HP Ethernet 1Gb 4-port 331i Adapter (22BE)
- HP Ethernet 1Gb 4-port 331FLR Adapter
- HP Ethernet 1Gb 4-port 331T Adapter
- HP Ethernet 1Gb 2-port 332i Adapter (2133)
- HP Ethernet 1Gb 2-port 332i Adapter (22E8)
- HP Ethernet 1Gb 2-port 332T Adapter

HPE Intel esx-provider for VMware
Version: 2018.06.04 **(Optional)**
Filename: cp034087.compsig; cp034087.zip
Driver Name and Version:

Enhancements

This product now supports vmkliux and native driver architectures.

Supported Devices and Features

These drivers support the following network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter
- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter
- HP Ethernet 10Gb 2-port 562FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 562SFP+ Adapter

HPE ProLiant Converged Network Utility for Windows Server x64 Editions
Version: 5.2.3.1 **(Optional)**
Filename: cp030269.exe

Enhancements

This product now supports Windows Server 2016.

This product now supports the following network adapters:

- HP Flex-10 10Gb 2-port 530M Adapter
- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HPE Ethernet 4x25Gb 1-port 620QSFP28 Adapter
- HPE Synergy 10Gb 2-port 2820C Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

This product now provides Fibre-Channel over Ethernet N-port ID Virtualization (FCoE NPIV) configuration for following network adapters:

- HP Flex-10 10Gb 2-port 530M Adapter
- HP FlexFabric 10Gb 2-port 533FLR-T Adapter

- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534FLB Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HP FlexFabric 10Gb 2-port 536FLB Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Adapter
- HPE StoreFabric CN1200E-T Adapter
- HPE Synergy 10Gb 2-port 2820C Converged Network Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

This product now fully supports the IPv4 Dynamic Host Configuration Protocol (DHCP).

This product now provides a OneView detection mechanism.

Supported Devices and Features

This software supports the following network adapters:

- HP Flex-10 10Gb 2-port 530M Adapter
- HP Ethernet 10Gb 2-port 530SFP+ Adapter
- HP Ethernet 10Gb 2-port 530T Adapter
- HP FlexFabric 10Gb 2-port 533FLR-T Adapter
- HP FlexFabric 10Gb 2-port 534FLB Adapter
- HP FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter
- HP FlexFabric 10Gb 2-port 534M Adapter
- HPE FlexFabric 10Gb 4-port 536FLR-T Adapter
- HPE FlexFabric 10Gb 2-port 556FLB Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HP Ethernet 10Gb 2-port 557SFP+ Adapter
- HPE Ethernet 25Gb 4-port 620SFP28 Adapter
- HP FlexFabric 20Gb 2-port 630FLB Adapter
- HP FlexFabric 20Gb 2-port 630M Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Converged Network Adapter
- HPE StoreFabric CN1200E-T Adapter
- HPE Synergy 10Gb 2820C Ethernet Adapter
- HPE Synergy 3820C 10/20Gb Converged Network Adapter

Intel Active Health System Agent for HPE ProLiant Network Adapters for Linux x86_64
Version: 1.1.83.0-1 (B) **(Optional)**
Filename: hp-ocsbbd-1.1.83.0-1.x86_64.compsig; hp-ocsbbd-1.1.83.0-1.x86_64.rpm; hp-ocsbbd-1.1.83.0-1.x86_64.txt

Fixes

SUM no longer attempts to install this product on Gen10 servers, which this product does not support.

Supported Devices and Features

This software supports the following Intel network adapters:

- HP Ethernet 1Gb 2-port 361i Adapter
- HP Ethernet 1Gb 2-port 361T Adapter
- HP Ethernet 1Gb 2-port 363i Adapter
- HP Ethernet 1Gb 2-port 364i Adapter
- HP Ethernet 1Gb 4-port 366FLR Adapter
- HP Ethernet 1Gb 4-port 366M Adapter
- HP Ethernet 1Gb 4-port 366T Adapter
- HP Ethernet 10Gb 2-port 560FLB Adapter
- HP Ethernet 10Gb 2-port 560FLR-SFP+ Adapter
- HP Ethernet 10Gb 2-port 560M Adapter
- HP Ethernet 10Gb 2-port 560SFP+ Adapter
- HP Ethernet 10Gb 2-port 561FLR-T Adapter
- HP Ethernet 10Gb 2-port 561T Adapter

Software - Storage Controller Top

HPE ProLiant Smart Array SAS/SATA Event Notification Service for 64-bit Windows Server Editions

Version: 6.46.0.64 (D) **(Optional)**
Filename: cp034046.exe

Enhancements

Added support for Microsoft Windows 10

HPE Smart Array SR Event Notification Service for Windows Server 64-bit Editions
Version: 1.0.0.64 (B) **(Recommended)**
Filename: cp034018.compsig; cp034018.exe

Enhancements

Added support for Microsoft Windows 10

Software - Storage Fibre Channel Top

Emulex Fibre Channel driver component for VMware vSphere 6.0
Version: 2018.06.01 **(Recommended)**
Filename: cp034222.compsig; cp034222.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Fixes

Fixed the following:

- unexpected behavior with incomplete path reporting that would cause an unexpectedly high number of dropped frames reported by the target and driver
- driver abort request to properly abort ELS (Extended Link Services) command

Enhancements

Updated to driver version 11.4.329.0

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

Emulex Fibre Channel driver component for VMware vSphere 6.5
Version: 2018.06.01 **(Recommended)**
Filename: cp034223.compsig; cp034223.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Fixes

Fixed the following:

- unexpected behavior with incomplete path reporting that would cause an unexpectedly high number of dropped frames reported by the target and driver
- driver abort request to properly abort ELS (Extended Link Services) command

Enhancements

Updated to driver version 11.4.329.0

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

Emulex(BRCM) Fibre Channel Over Ethernet driver for VMware vSphere 6.0
Version: 2018.06.01 **(Recommended)**
Filename: cp034209.compsig; cp034209.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals

2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to Driver version 12.0.1115.0

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HPE StoreFabric CN1200E-T Adapter

Emulex(BRCM) Fibre Channel over Ethernet driver for VMware vSphere 6.5
Version: 2018.06.01 **(Recommended)**
Filename: cp034210.compsig; cp034210.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to Driver version 12.0.1115.0

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HPE StoreFabric CN1200E-T Adapter

QLogic Fibre Channel driver component for VMware vSphere 6.0
Version: 2018.06.01 **(Recommended)**
Filename: cp034226.compsig; cp034226.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Fixes

This driver version resolves the following:

- Driver is selecting to run LB (Loopback) rather than echo for F_Port
- If the SNS (Storage Name Service) fabric login appears incomplete, it would not be retried.
- If switch domain controller continuously tries to login, there exists a window where driver database and firmware database can go out of sync causing fabric discovery incomplete, and the login retry count is exhausted.
- The driver does not report minimum speeds correctly for 16G and 32G adapters.
- Echo ELS (Extended Link Services) test using QCC (QLogic Converge Console) CLI (Command Line Interface) was incomplete with invalid WWPN (World Wide Port Name) status.
- Re-login is being triggered too fast.
- Inquiry response snooping does not take into account the possibility of multiple scatter gather elements.
- Target devices are temporarily not accessible when the link toggle occurs on one of the target device paths.
- Driver would not send the full RDP (Read Diagnostic Parameter) response with a switch port that was not in the logged in state.
- Driver was advertising 1G speed support for 8G adapters.
- FDMI (Fabric Device Management Interface) info showing incorrect supported speeds for 16G mezzanine adapters in FDMI (Fabric Device Management Interface).

Enhancements

Driver version 2.1.73.0

Added support for the following:

- IOCB (I/O Control Block) based fabric priority per logged in FC (Fibre Channel) port.
- Enable Priority Tagging VM-ID (Virtual Machine Identification Data) support
- Update ISP25XX FW (Firmware) to version 8.07.00
- End-to-End QoS (Quality of Service) fabric priority support

Supported Devices and Features

This driver supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

QLogic Fibre Channel driver component for VMware vSphere 6.5
Version: 2018.06.01 **(Recommended)**
Filename: cp034227.compsig; cp034227.zip
Driver Name and Version:

Important Note!

This component is intended to be used by HPE applications. It is a zip that contains the same driver deliverable available from the vmware.com and the HPE vibsdepot.hpe.com webpages, plus an HPE specific CPXXXX.xml file.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Fixes

This driver verson resolves the following:

- Driver is selecting to run LB (Loopback) rather than echo for F_Port
- If the SNS (Storage Name Service) fabric login appears incomplete, it would not be retried.
- If switch domain controller continuously tries to login, there exists a window where driver database and firmware database can go out of sync causing fabric discovery incomplete, and the login retry count is exhausted.
- The driver does not report minimum speeds correctly for 16G and 32G adapters.
- Echo ELS (Extended Link Services) test using QCC (QLogic Converge Console) CLI (Command Line Interface) was incomplete with invalid WWPN (World Wide Port Name) status.
- Re-login is being triggered too fast.
- Inquiry response snooping does not take into account the possibility of multiple scatter gather elements.
- Target devices are temporarily not accessible when the link toggle occurs on one of the target device paths.
- Driver would not send the full RDP (Read Diagnostic Parameter) response with a switch port that was not in the logged in state.
- Driver was advertising 1G speed support for 8G adapters.
- FDMI (Fabric Device Management Interface) info showing incorrect supported speeds for 16G mezzanine adapters in FDMI (Fabric Device Management Interface).

Enhancements

Driver version 2.1.73.0

Added support for the following:

- IOCB (I/O Control Block) based fabric priority per logged in FC (Fibre Channel) port.
- Enable Priority Tagging VM-ID (Virtual Machine Identification Data) support
- Update ISP25XX FW (Firmware) to version 8.07.00
- End-to-End QoS (Quality of Service) fabric priority support

Supported Devices and Features

This driver supports the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

Software - Storage Fibre Channel HBA [Top]

Fibreutils for HPE Storage Fibre Channel Host Bus Adapters for Linux (x86_64)
Version: 3.3-5 **(Optional)**
Filename: fibreutils-3.3-5.x86_64.compsig; fibreutils-3.3-5.x86_64.rpm

Prerequisites

- Requires the following packages to be installed: glibc libgcc libstdc++ bash perl

Enhancements

Updated code for the following:

- Emulex CNA Driver display due to split
- Optrom version display

HPE Emulex Fibre Channel Enablement Kit for Red Hat Enterprise Linux 6 Server
Version: 11.4.334.2 **(Recommended)**
Filename: HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.rhel6.x86_64.compsig; HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.rhel6.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

The target environment must have the libHBAAPI Package installed prior to the installation of the enablement kit. (If not already present, the libHBAAPI Package can be obtained from the operating system installation media.)

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to version 11.4.334.2

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class

HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

HPE Emulex Fibre Channel Enablement Kit for Red Hat Enterprise Linux 7 Server
Version: 11.4.334.2 **(Recommended)**
Filename: HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.rhel7.x86_64.compsig; HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.rhel7.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

The target environment must have the libHBAAPI Package installed prior to the installation of the enablement kit. (If not already present, the libHBAAPI Package can be obtained from the operating system installation media.)

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Added support to Red Hat Enterprise Linux 7u5

Updated to version 11.4.334.2

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter

- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

HPE Emulex Fibre Channel Enablement Kit for SUSE Linux Enterprise Server 11 (AMD64/EM64T)
Version: 11.4.334.2 **(Recommended)**
Filename: HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.sles11sp3.x86_64.compsig; HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.sles11sp3.x86_64.rpm; HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.sles11sp4.x86_64.compsig; HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.sles11sp4.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

The target environment must have the libHBAAPI Package installed prior to the installation of the enablement kit. (If not already present, the libHBAAPI Package can be obtained from the operating system installation media.)

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to version 11.4.334.2

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter

- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

HPE Emulex Fibre Channel Enablement Kit for SUSE Linux Enterprise Server 12
Version: 11.4.334.2 **(Recommended)**
Filename: HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.sles12sp2.x86_64.compsig; HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.sles12sp2.x86_64.rpm; HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.sles12sp3.x86_64.compsig; HP-CNA-FC-Emulex-Enablement-Kit-11.4.334.2-1.sles12sp3.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

The target environment must have the libHBAAPI Package installed prior to the installation of the enablement kit. (If not already present, the libHBAAPI Package can be obtained from the operating system installation media.)

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to version 11.4.334.2

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter

- HP LPe1205A 8Gb Fibre Channel Host Bus Adapter for BladeSystem c-Class
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

HPE Emulex Smart SAN Enablement Kit for Linux
Version: 1.0.0.0-4 (b) **(Optional)**
Filename: hpe-emulex-smartsan-enablement-kit-1.0.0.0-4.x86_64.compsig; hpe-emulex-smartsan-enablement-kit-1.0.0.0-4.x86_64.rpm

Important Note!

To obtain the 3PAR Smart SAN User Guide to go the Storage Information Library at the following link:

Storage Information Library

(http://www.hpe.com/info/storage/docs/)

By default, **HP 3PAR Storage** is selected under

Products and Solutions.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied fibre channel driver must be installed prior to this enablement kit component if you want to enable Smart SAN functionality. The driver is available on the HPE.com website at www.hpe.com.

Linux FC Driver Kit for HPE Branded Emulex FC HBAs and mezz cards, version 11.1.183.21, for RedHat 6, RedHat 7, and Novell SUSE 11, SUSE 12

However, if a Smart SAN enabled driver is not installed at execution time, the component will land the enablement kit files for future use after the driver has been installed.

Enhancements

Updated to version 1.0.0.0-4 (b)

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA

- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

HPE Emulex Smart SAN Enablement Kit for Windows 64 bit operating systems
Version: 1.0.0.1 (f) **(Optional)**
Filename: cp033240.compsig; cp033240.exe

Important Note!

The Smart SAN enablement kit will not execute when an operating system has only the inbox fibre channel driver installed. An out of box (OOB) fibre channel driver is needed to utilize Smart SAN functionality. If any OOB driver is installed, the enablement kit will pre-enable/disable Smart SAN functionality for future use. It can then be activated once a Smart SAN enabled OOB driver is installed (see Prerequisite Notes) and after a reboot has occured.

To obtain the 3PAR Smart SAN User Guide to go the Storage Information Library at the following link:

Storage Information Library

(http://www.hpe.com/info/storage/docs/)

By default, **HP 3PAR Storage** is selected under

Products and Solutions.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied fibre channel driver must be installed prior to this enablement kit component if you want to enable Smart SAN functionality. The driver is available on the HPE.com website at www.hpe.com.

HPE Storage Fibre Channel Adapter Kit for the x64 Emulex Storport Driver v11.1.145.16 cp030886.exe

However, if a Smart SAN enabled driver is not installed at execution time, the component will land the enablement kit files for future use after the driver has been installed.

Enhancements

Updated to version 1.0.0.1 (f)

Supported Devices and Features

This component is supported on following Emulex Fibre Channel Host Bus adapters:

8Gb FC:

- HP 81E 8Gb Single Port PCIe Fibre Channel Host Bus Adapter
- HP 82E 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric 84E 4-Port Fibre Channel Host Bus Adapter

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1000E 16Gb Single Port Fibre Channel Host Bus Adapter
- HP Fibre Channel 16Gb LPe1605 Mezz
- HP SN1100E 16Gb Dual Port Fibre Channel Host Bus Adapter
- HP SN1100E 16Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1100E 4P 16Gb Fibre Channel Host Bus Adapter
- HPE Synergy 3530C 16Gb Fibre Channel Host Bus Adapter

LPe31000/32000 (16Gb/32Gb) FC:

- HPE StoreFabric SN1200E 16Gb 2P FC HBA
- HPE StoreFabric SN1200E 16Gb 1P FC HBA
- HPE StoreFabric SN1600E 32Gb 2p FC HBA
- HPE StoreFabric SN1600E 32Gb 1p FC HBA

HPE Emulex(BRCM) Fibre Channel Over Ethernet Enablement Kit for Red Hat Enterprise Linux 6 Server
Version: 12.0.1107.0 **(Recommended)**
Filename: HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.rhel6.x86_64.compsig; HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.rhel6.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

The target environment must have the libHBAAPI Package installed prior to the installation of the enablement kit. (If not already present, the libHBAAPI Package can be obtained from the operating system installation media.)

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to version: 12.0.1107.0

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex(BRCM) Fibre Channel Over Ethernet Enablement Kit for Red Hat Enterprise Linux 7 Server
Version: 12.0.1107.0 **(Recommended)**
Filename: HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.rhel7.x86_64.compsig; HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.rhel7.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

The target environment must have the libHBAAPI Package installed prior to the installation of the enablement kit. (If not already present, the libHBAAPI Package can be obtained from the operating system installation media.)

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Added support to Red Hat Enterprise Linux 7u5

Updated to version: 12.0.1107.0

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex(BRCM) Fibre Channel Over Ethernet Enablement Kit for SUSE Linux Enterprise Server 11 (AMD64/EM64T)
Version: 12.0.1107.0 **(Recommended)**
Filename: HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.sles11sp3.x86_64.compsig; HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.sles11sp3.x86_64.rpm; HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.sles11sp4.x86_64.compsig; HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.sles11sp4.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

The target environment must have the libHBAAPI Package installed prior to the installation of the enablement kit. (If not already present, the libHBAAPI Package can be obtained from the operating system installation media.)

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to version: 12.0.1107.0

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE Emulex(BRCM) Fibre Channel Over Ethernet Enablement Kit for SUSE Linux Enterprise Server 12
Version: 12.0.1107.0 **(Recommended)**
Filename: HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.sles12sp2.x86_64.compsig; HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.sles12sp2.x86_64.rpm; HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.sles12sp3.x86_64.compsig; HP-CNA-FC-Broadcom-Enablement-Kit-12.0.1107.0-1.sles12sp3.x86_64.rpm

Important Note!

Release Notes:
HPE StoreFabric Emulex Adapters Release Notes

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Prerequisites

The target environment must have the libHBAAPI Package installed prior to the installation of the enablement kit. (If not already present, the libHBAAPI Package can be obtained from the operating system installation media.)

Beginning with software release 11.2, Fibre Channel (LightPulse) adapters and Converged Network adapters (OneConnect) have independent software kits.

It is highly recommended that you review the Broadcom Software Kit Migration User Guide for more detailed information regarding this change.

To obtain the guide:

1. Go to http://www.hpe.com/support/manuals
2. Using the HPE model number as your guide, enter the adapter model number in the Search products box, and then click >>.

This document provides special instructions and considerations for using the driver kits for FC and CNA adapters.

Special cases include those in which pre-11.2 (original) drivers and applications are replaced by the new 11.2 drivers and applications, and cases in which inbox drivers are replaced by the new 11.2 out-of-box (OOB) drivers.

Enhancements

Updated to version: 12.0.1107.0

Supported Devices and Features

This component is supported on following Emulex Converged Network Adapters:

XE100 Series:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2-port 650FLB Adapter
- HP FlexFabric 20Gb 2-port 650M Adapter
- HP FlexFabric 10Gb 2-port 556FLR-SFP+ Adapter
- HPE FlexFabric 10Gb 2-port 556FLR-T Adapter
- HPE StoreFabric CN1200E-T Adapter

HPE QLogic Fibre Channel Enablement Kit for Linux
Version: 6.0.0.0-4 (d) **(Optional)**
Filename: HP-CNA-FC-hpqlgc-Enablement-Kit-6.0.0.0-4.noarch.compsig; HP-CNA-FC-hpqlgc-Enablement-Kit-6.0.0.0-4.noarch.rpm

Important Note!

Release Notes:
HPE StoreFabric QLogic Adapters Release Notes

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

Enhancements

Updated the kit to version 6.0.0.0-4

Supported Devices and Features

This version of the enablement kit supports the following devices:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA
- HP QMH2572 8Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

HPE QLogic Smart SAN enablement kit for Linux
Version: 3.3-3 (b) **(Optional)**
Filename: hpe-qlogic-smartsan-enablement-kit-3.3-3.x86_64.compsig; hpe-qlogic-smartsan-enablement-kit-3.3-3.x86_64.rpm

Important Note!

To obtain the 3PAR Smart SAN User Guide to go the Storage Information Library at the following link:

Storage Information Library

(http://www.hpe.com/info/storage/docs/)

By default, **HP 3PAR Storage** is selected under

Products and Solutions.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied fibre channel driver must be installed prior to this enablement kit component if you want to enable Smart SAN functionality. The driver is available on the HPE.com website at www.hpe.com.

- Red Hat Enterprise Linux 6 Server (x86-64) FCoE/FC Driver Kit for HPE Qlogic CNAs, HBAs and mezzanine HBAs, version 8.07.00.42.06.0-k1
- Red Hat Enterprise Linux 7 Server FCoE/FC Driver Kit for HPE QLogic CNAs, HBAs and mezzanine HBAs and CNAs, version 8.07.00.42.07.0-k1
- SUSE Linux Enterprise Server 11 (AMD64/EM64T) FCoE/FC Driver Kit for HPE Qlogic CNAs, HBAs and mezzanine HBAs, version 8.07.00.42.11.3-k
- SUSE Linux Enterprise Server 12 FCoE/FC Driver Kit for HPE QLogic CNAs, HBAs and mezzanine HBAs and CNAs version 8.07.00.42.12.0-k1

However, if a Smart SAN enabled driver is not installed at execution time, the component will land the enablement kit files for future use after the driver has been installed.

Enhancements

Updated to version 3.3-3(b)

Supported Devices and Features

This enablement kit is supported on the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

HPE QLogic Smart SAN Enablement Kit for Windows 64 bit operating systems
Version: 1.0.0.1 (e) **(Optional)**
Filename: cp033239.compsig; cp033239.exe

Important Note!

The Smart SAN enablement kit will not execute when an operating system has only the inbox fibre channel driver installed. An out of box (OOB) fibre channel driver is needed to utilize Smart SAN functionality. If any OOB driver is installed, the enablement kit will pre-enable/disable Smart SAN functionality for future use. It can then be activated once a Smart SAN enabled OOB driver is installed (see Prerequisite Notes) and after a reboot has occured.

To obtain the 3PAR Smart SAN User Guide to go the Storage Information Library at the following link:

Storage Information Library

(http://www.hpe.com/info/storage/docs/)

By default, **HP 3PAR Storage** is selected under

Products and Solutions.

Prerequisites

Please consult SPOCK for a list of supported configurations available at the following link:

http://www.hpe.com/storage/spock/

The HPE supplied fibre channel driver must be installed prior to this enablement kit component if you want to enable Smart SAN functionality. The driver is available on the HPE.com website at www.hpe.com.

- HPE Storage Fibre Channel Adapter Kit for the x64 QLogic Storport Driver v9.2.2.20, cp031252.exe
- HPE Storage Fibre Channel Adapter Kit for the QLogic Storport Driver for Windows Server 2012 and 2012 R2 v9.2.2.20, cp031253.exe
- HPE Storage Fibre Channel Adapter Kit for the QLogic Storport Driver for Windows Server 2016 version 9.2.2.20, cp031251.exe

However, if a Smart SAN enabled driver is not installed at execution time, the component will land the enablement kit files for future use after the driver has been installed.

Enhancements

Updated to version 1.0.0.1 (e)

Supported Devices and Features

This enablement kit is supported on the following HPE adapters:

8Gb FC:

- HP 81Q PCIe Fibre Channel Host Bus Adapter
- HP 82Q 8Gb Dual Port PCIe Fibre Channel Host Bus Adapter
- HPE StoreFabric 84Q 4P 8Gb Fibre Channel HBA

16Gb FC:

- HP QMH2672 16Gb Fibre Channel Host Bus Adapter for c-Class BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1000Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 2-port PCIe Fibre Channel Host Bus Adapter
- HP StoreFabric SN1100Q 16GB 1-port PCIe Fibre Channel Host Bus Adapter
- HPE Synergy 3830C 16G Fibre Channel Host Bus Adapter

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Port Fibre Channel Host Bus Adapter
- HPE StoreFabric SN1600Q 32Gb Dual Port Fibre Channel Host Bus Adapter

---

Software - System Management Top

Agentless Management Service (iLO 5) for Red Hat Enterprise Linux 6 Server
Version: 1.3.0 **(Optional)**
Filename: amsd-1.3.0-2803.25.rhel6.x86_64.compsig; amsd-1.3.0-2803.25.rhel6.x86_64.rpm

Prerequisites

- **amsd only supported on HPE ProLiant Gen10 Servers.**
- **amsd provides information to the iLO 5 service providing SNMP support.**
- **SNMP PASS-THRU on the iLO 5 MUST be disabled, and SNMP should be configured on the iLO 5. The iLO 5 may need to be reset after changing these settings.**
- **Requirements:**
  - Minimum iLO 5 Firmware Version = 1.1
  - Minimum supported OS Versions = Red Hat Enterprise Linux 6.9

Fixes

Fixed the following items:

- Better LSB conformance for startup/shutdown scripts
- Improve support for multiple SNMP AgentX sub-agents
- Improved detection of LogMapSpeedMbps for drivers that do not support NIC speeds in sysfs
- Improved support for HPE Smart Array P824i-p MegaRAID SAS controller including support for logical drives
- Added checks to ahslog to prevent it from sending too large requests to the iLO
- Fixed incorrect cpqNicIfLogMapAdapterOKCount for simple NIC logical devices

Enhancements

New features of amsd version 1.3.0:

- iSCSI support in the cpqiScsi MIB handler

- Add volume usage to ahslog
- Add NIC link monitoring to ahslog

Agentless Management Service (iLO 5) for Red Hat Enterprise Linux 7 Server
Version: 1.3.0 **(Optional)**
Filename: amsd-1.3.0-2804.29.rhel7.x86_64.compsig; amsd-1.3.0-2804.29.rhel7.x86_64.rpm

Prerequisites

- **amsd only supported on HPE Gen10 Servers.**
- **amsd provides information to the iLO 5 service providing SNMP support.**
- **SNMP PASS-THRU on the iLO 5 MUST be disabled, and SNMP should be configured on the iLO 5. The iLO 5 may need to be reset after changing these settings.**
- **Requirements:**
  - Minimum iLO 5 Firmware Version = 1.1
  - Minimum supported OS Versions = Red Hat Enterprise Linux 7.3 Errata 3.10.0.514.6.1

Fixes

Fixed the following items:

- Fix libpci dependencies for amsd installation on Red Hat Enterprise Linux 7.2
- Better LSB conformance for startup/shutdown scripts
- Improve support for multiple SNMP AgentX sub-agents
- Improved detection of LogMapSpeedMbps for drivers that do not support NIC speeds in sysfs
- Improved support for HPE Smart Array P824i-p MegaRAID SAS controller including support for logical drives
- Added checks to ahslog to prevent it from sending too large requests to the iLO
- Fixed incorrect cpqNicIfLogMapAdapterOKCount for simple NIC logical devices

Enhancements

New features of amsd version 1.3.0:

- iSCSI support in the cpqiScsi MIB handler
- Add volume usage to ahslog
- Add NIC link monitoring to ahslog

Agentless Management Service (iLO 5) for SUSE Linux Enterprise Server 11
Version: 1.3.0 **(Optional)**
Filename: amsd-1.3.0-2804.23.sles11.x86_64.compsig; amsd-1.3.0-2804.23.sles11.x86_64.rpm

Prerequisites

- **amsd only supported on HPE Gen10 Servers.**
- **amsd provides information to the iLO 5 service providing SNMP support.**
- **SNMP PASS-THRU on the iLO 5 MUST be disabled, and SNMP should be configured on the iLO 5. The iLO 5 may need to be reset after changing these settings.**
- **Requirements:**

  Minimum iLO 5 Firmware Version = 1.1

  Minimum supported OS Versions = SuSE Linux Enterprise Server 11 SP4 kISO

Fixes

Fixed the following items:

- Better LSB conformance for startup/shutdown scripts
- Improve support for multiple SNMP AgentX sub-agents
- Improved detection of LogMapSpeedMbps for drivers that do not support NIC speeds in sysfs
- Improved support for HPE Smart Array P824i-p MegaRAID SAS controller including support for logical drives
- Added checks to ahslog to prevent it from sending too large requests to the iLO
- Fixed incorrect cpqNicIfLogMapAdapterOKCount for simple NIC logical devices

Enhancements

New features of amsd version 1.3.0:

- iSCSI support in the cpqiScsi MIB handler

- Add volume usage to ahslog
- Add NIC link monitoring to ahslog

Agentless Management Service (iLO 5) for SUSE Linux Enterprise Server 12
Version: 1.3.0 **(Optional)**
Filename: amsd-1.3.0-2804.23.sles12.x86_64.compsig; amsd-1.3.0-2804.23.sles12.x86_64.rpm

Prerequisites

- **amsd only supported on HPE Gen10 Servers.**
- **amsd provides information to the iLO 5 service providing SNMP support.**
- **SNMP PASS-THRU on the iLO 5 MUST be disabled, and SNMP should be configured on the iLO 5. The iLO 5 may need to be reset after changing these settings.**
- **Requirements:**
  - Minimum iLO 5 Firmware Version = 1.1
  - Minimum supported OS Versions = SuSE Linux Enterprise Server 12 SP2

Fixes

Fixed the following items:

- Better LSB conformance for startup/shutdown scripts
- Improve support for multiple SNMP AgentX sub-agents
- Improved detection of LogMapSpeedMbps for drivers that do not support NIC speeds in sysfs
- Improved support for HPE Smart Array P824i-p MegaRAID SAS controller including support for logical drives
- Added checks to ahslog to prevent it from sending too large requests to the iLO
- Fixed incorrect cpqNicIfLogMapAdapterOKCount for simple NIC logical devices

Enhancements

New features of amsd version 1.3.0:

- iSCSI support in the cpqiScsi MIB handler
- Add volume usage to ahslog
- Add NIC link monitoring to ahslog

Agentless Management Service for Windows X64
Version: 1.30.0.0 **(Optional)**
Filename: cp034101.compsig; cp034101.exe

Important Note!

About installation and enablement of SMA service:

- During AMS installation in interactive mode, there is pop up message to selectively install SMA.
  - If Yes is selected, SMA service will be installed and set to running state.
  - If No is selected, SMA service will be installed but the service is not enabled.
- During AMS installation in silent mode, SMA is installed but the service is not enabled.
- To enable SMA service at a later time, go to the following folder: %ProgramFiles%\OEM\AMS\Service\ (Typically c:\Program Files\OEM\AMS\Service) and execute "EnableSma.bat /f"
- IMPORTANT: The SNMP service community name and permission must be also be setup. This is not done by “EnableSma.bat”. To
- disable SMA after it has been enabled, go the the following folder: %ProgramFiles%\OEM\AMS\Service\ (Typically c:\Program Files\OEM\AMS\Service) and execute "DisableSma.bat /f"
- After installing Windows operating system, make sure all the latest Microsoft Updates are downloaded and installed (wuapp.exe can be launched to start the update process). If this is not done, a critical error may be reported in Windows Event Log, “The Agentless Management Service terminated unexpectedly.”.

AMS Control Panel Applet:

- The AMS control panel applet UI is best displayed on the system when screen resolution is 1280 x 1024 pixels or higher and text size 100%.

Prerequisites

The *Channel Interface Driver for Windows X64* must be installed prior to this component.

Microsoft SNMP Service must be enabled, if SMA (System Management Assistant) is enabled.

Fixes

- AMS service no longer terminates unexpectedly if the server had more than 9 IPV6 addresses. However, cpqNicIfLogMapIPV6Address OID will only return up to 9 IPV6 addresses.
- Traps 1015, 1019,1020 now have correct varbind info, consistent with MIB definitions.
- When SMA (System Management Assistant) service is stopped or disabled, SMA will no longer respond to SNMP queries with outdated data.

Enhancements

- Added support for the following IO devices:
  - HPE Synergy 4820C 10/20/25Gb Converged Network Adapter
  - HPE StorFabric CN1200R-T Converged Network Adapter
  - HPE StorFabric CN1300R Converged Network Adapter
  - HPE Synergy 6410C 25/50Gb Ethernet Adapter
  - HPE Ethernet 100Gb 1-port 842QSFP28 Adapter
  - HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFP Adapter
- Added the following enhancements to Control Panel Applet:
  - Up to 8 trap destinations are supported in SNMP tab, along with user configuration and SNMPv3 settings
  - SNMP tab is now fully functional if iLO5 encryption is set to HighSecurity or FIPS mode
  - Button options are available to start, stop, enable or disable SMA service
  - GUI options are available to select time format and input the optional periodic test trap interval
  - Help content has expanded
- SMA (System Management Assistant) service now supports all MIB OIDs and traps generated by iLO5 FW.
- Added support for System Chassis Class of IML Events in Windows Event Log.
- iSCSI MIB condition is now available in cpqHoMibHealthStatusArray.
- AHS (Active Health System) NIC Link records now contain Interface Description string.

HPE ESXi Offline Bundle for VMware vSphere 6.0
Version: 3.3.0 **(Recommended)**
Filename: esxi6.0uX-mgmt-bundle-3.3.0-11.zip

Fixes

WBEM Providers

- Fixed issue with Smart Array Provider reporting change of battery status frequently

Agentless Management Service

- Fixed to remove heartbeat trap (cpqHo2GenericTrap) delivery at OS boot when periodic test trap feature is disabled
- Fixed memory leak partly caused by AMS running in the OS init resource group
- Fixed reporting of the embedded SATA controller to resolve missing drives in the iLO Storage Tab display

Enhancements

WBEM Providers

- Added support for Smart Array Controller model P408i-sb

Agentless Management Service

- Added reporting of OS Logical Disk Volume Configuration and Utilization to iLO's Active Health System Log

Supported Devices and Features

VMware vSphere version support:

- VMware vSphere 6.0 U2
- VMware vSphere 6.0 U3

HPE ESXi Offline Bundle for VMware vSphere 6.5
Version: 3.3.0 **(Recommended)**
Filename: esxi6.5uX-mgmt-bundle-3.3.0-10.zip

Fixes

WBEM Providers

- Fixed issue with Smart Array Provider reporting change of battery status frequently

Agentless Management Service

- Fixed to remove heartbeat trap (cpqHo2GenericTrap) delivery at OS boot when periodic test trap feature is disabled
- Fixed memory leak partly caused by AMS running in the OS init resource group
- Fixed reporting of the embedded SATA controller to resolve missing drives in the iLO Storage Tab display

Enhancements

WBEM Providers

- Added support for Smart Array Controller model P408i-sb

Agentless Management Service

- Added reporting of OS Logical Disk Volume Configuration and Utilization to iLO's Active Health System Log

Supported Devices and Features

VMware vSphere version support:

- VMware vSphere 6.5 U1
- VMware vSphere 6.5 U2

HPE ESXi Utilities Offline Bundle for VMware vSphere 6.0
Version: 3.3.0 **(Recommended)**
Filename: esxi6.0-util-bundle-3.3.0-8.zip

Important Note!

Refer to the HPE VMware Utilities Guide for VMware vSphere 6.0 for June 2018 which is located at www.hpe.com/info/vmware/proliant-docs.

Enhancements

Updated the Smart Storage Array Command Line Interface (SSACLI) utility

---

HPE ESXi Utilities Offline Bundle for VMware vSphere 6.5
Version: 3.3.0 **(Recommended)**
Filename: esxi6.5-util-bundle-3.3.0-8.zip

Important Note!

Refer to the HPE VMware Utilities Guide for VMware vSphere 6.5 for June 2018 which is located at www.hpe.com/info/vmware/proliant-docs.

Enhancements

Updated the Smart Storage Administrator CLI (SSACLI)

HPE Insight Management Agents for Windows Server x64 Editions
Version: 10.90.0.0 **(Optional)**
Filename: cp035320.exe

Prerequisites

The HPE Insight Management Agents require the SNMP Service , HPE ProLiant iLO 3/4 Channel Interface and Management Controller Drivers for Windows x64 to be installed prior to this component.

In addition, the System Management Homepage (SMH) component is required for a single server web-based user interface.

Fixes

- The accelerator status changed to permanent disabled event information on storage agents
- Software Versions Agent triggers McAfee VSE Access Protection Violation

---

HPE Insight Management WBEM Providers for Windows Server x64 Editions
Version: 10.70.0.0 **(Optional)**
Filename: cp033066.exe

Important Note!

Version 10.70.0.0 will be the last HPE Insight Management WBEM Providers release to support Gen9 servers.

Prerequisites

The HPE Insight Management WBEM Providers require the HPE ProLiant iLO 3/4 Channel Interface and Management Controller Drivers (version 3.4.0.0 or later) for Windows X64 to be installed prior to this component.

In addition, the System Management Homepage (SMH) component (version 7.2.2.9 or later) is required for a single server web-based user interface.

Fixes

Fixed a handle leak caused by Storage provider (hpwmisa.dll).

HPE MegaRAID Storage Administrator (HPE MRSA) for Linux 64-bit
Version: 3.91.0.0 **(Optional)**
Filename: HPE_Linux_64_readme.txt; MRStorageAdministrator-003.091.000.000-00.x86_64.rpm; MRStorageAdministrator-003.091.000.000-00.x86_64_part1.compsig; MRStorageAdministrator-003.091.000.000-00.x86_64_part2.compsig; MRStorageAdministrator-003.091.000.000-00.x86_64_part3.compsig; MRStorageAdministrator-003.091.000.000-00.x86_64_part4.compsig

Prerequisites

.

Enhancements

- Initial Release

HPE MegaRAID Storage Administrator (HPE MRSA) for Windows 64-bit
Version: 3.92.0.0 (B) **(Optional)**
Filename: cp035098.exe; cp035098_part1.compsig; cp035098_part2.compsig; cp035098_part3.compsig; cp035098_part4.compsig

Enhancements

- Added HPE Digital Signature

HPE MegaRAID Storage Administrator StorCLI for Linux 64-bit
Version: 1.24.09 **(Optional)**
Filename: LINUX_Readme.txt; storcli-1.24.09-1.noarch.compsig; storcli-1.24.09-1.noarch.rpm

Enhancements

- Initial Release

HPE MegaRAID Storage Administrator StorCLI for Windows 64-bit
Version: 1.24.9.0 (B) **(Optional)**
Filename: cp035244.compsig; cp035244.exe

Important Note!

- Customers who already have firmware version 1.24.9.0 installed do not need to update to 1.24.9.0(B).

Enhancements

- Added HPE Digital Signature

HPE ProLiant Agentless Management Service for HPE Apollo, ProLiant and Synergy Gen9 servers
Version: 10.90.0.0 **(Optional)**
Filename: cp034100.exe

Prerequisites

The *HPE ProLiant iLO 3/4 Channel Interface Driver for Windows X64* (version 3.4.0.0 or later) must be installed prior to this component.

Fixes

- AMS service no longer terminates unexpectedly if the server had more than 9 IPV6 addresses. However, cpqNicIfLogMapIPV6Address OID will only return up to 9 IPV6 addresses.
- Traps 1015, 1019,1020 now have correct varbind info, consistent with MIB definitions.

HPE ProLiant Agentless Management Service for Red Hat Enterprise Linux 6 (AMD64/EM64T)
Version: 2.8.0 **(Optional)**
Filename: hp-ams-2.8.0-2861.27.rhel6.x86_64.compsig; hp-ams-2.8.0-2861.27.rhel6.x86_64.rpm

Prerequisites

- **hp-ams only supported on HP ProLiant Gen8 and Gen9 Servers.**
- **hp-ams provides information to the HP iLO 4 service providing SNMP support.**
- **SNMP PASS-THRU on the HP iLO 4 MUST be disabled, and SNMP should be configured on the HP iLO 4. The HP iLO 4 may need to be reset after changing these settings.**
- **Requirements:**
  - Minimum HP iLO 4 Firmware Version = 1.05
  - Minimum supported OS Versions = Red Hat Enterprise Linux 5.6, Red Hat Enterprise Linux 6.0, SuSE Linux Enterprise Server 10 SP4, SuSE Linux Enterprise Server 11 SP1

Fixes

Fixed the following items:

- When NIC bonding is configured; addressed issue where information was not displayed correctly within hp-ams
- Prioritized VLAN interfaces before Ethernet interfaces to correctly obtain the fibre channel controller information within hp-ams
- Ensure the proper bounds are validated before releasing memory with Scandir

---

HPE ProLiant Agentless Management Service for Red Hat Enterprise Linux 7 Server
Version: 2.8.0 **(Optional)**
Filename: hp-ams-2.8.0-2861.30.rhel7.x86_64.compsig; hp-ams-2.8.0-2861.30.rhel7.x86_64.rpm

Prerequisites

- **hp-ams supported on HP ProLiant Gen8 and Gen9 Servers.**
- **hp-ams provides information to the HP iLO 4 service providing SNMP support.**
- **SNMP PASS-THRU on the HP iLO 4 MUST be disabled, and SNMP should be configured on the HP iLO 4. The HP iLO 4 may need to be reset after changing these settings.**
- **Requirements:**
  - Minimum HP iLO 4 Firmware Version = 1.05
  - Minimum supported OS Versions = Red Hat Enterprise Linux 5.6, Red Hat Enterprise Linux 6.0, SuSE Linux Enterprise Server 10 SP4, SuSE Linux Enterprise Server 11 SP1

Fixes

Fixed the following items:

- Fix libpci dependencies for hp-ams installation on Red Hat Enterprise Linux 7.2
- When NIC bonding is configured; addressed issue where information was not displayed correctly within hp-ams
- Prioritized VLAN interfaces before Ethernet interfaces to correctly obtain the fibre channel controller information within hp-ams
- Ensure the proper bounds are validated before releasing memory with Scandir

---

HPE ProLiant Agentless Management Service for SUSE LINUX Enterprise Server 11 (AMD64/EM64T)
Version: 2.8.0 **(Optional)**
Filename: hp-ams-2.8.0-2861.27.sles11.x86_64.compsig; hp-ams-2.8.0-2861.27.sles11.x86_64.rpm

Prerequisites

- **hp-ams only supported on HP ProLiant Gen8 and Gen9 Servers.**
- **hp-ams provides information to the HP iLO 4 service providing SNMP support.**
- **SNMP PASS-THRU on the HP iLO 4 MUST be disabled, and SNMP should be configured on the HP iLO 4. The HP iLO 4 may need to be reset after changing these settings.**
- **Requirements:**
  - Minimum HP iLO 4 Firmware Version = 1.05
  - Minimum supported OS Versions = Red Hat Enterprise Linux 5.6, Red Hat Enterprise Linux 6.0, SuSE Linux Enterprise Server 10 SP4, SuSE Linux Enterprise Server 11 SP1

Fixes

Fixed the following items:

- When NIC bonding is configured; addressed issue where information was not displayed correctly within hp-ams
- Prioritized VLAN interfaces before Ethernet interfaces to correctly obtain the fibre channel controller information within hp-ams
- Ensure the proper bounds are validated before releasing memory with Scandir

---

HPE ProLiant Agentless Management Service for SUSE LINUX Enterprise Server 12
Version: 2.8.0 **(Optional)**

Filename: hp-ams-2.8.0-2861.27.sles12.x86_64.compsig; hp-ams-2.8.0-2861.27.sles12.x86_64.rpm

Prerequisites

- **hp-ams supported on HP ProLiant Gen8 and Gen9 Servers.**
- **hp-ams provides information to the HP iLO 4 service providing SNMP support.**
- **SNMP PASS-THRU on the HP iLO 4 MUST be disabled, and SNMP should be configured on the HP iLO 4. The HP iLO 4 may need to be reset after changing these settings.**
- **Requirements:**
  - Minimum HP iLO 4 Firmware Version = 1.05
  - Minimum supported OS Versions = Red Hat Enterprise Linux 5.6, Red Hat Enterprise Linux 6.0, SuSE Linux Enterprise Server 10 SP4, SuSE Linux Enterprise Server 11 SP1

Fixes

Fixed the following items:

- When NIC bonding is configured; addressed issue where information was not displayed correctly within hp-ams
- Prioritized VLAN interfaces before Ethernet interfaces to correctly obtain the fibre channel controller information within hp-ams
- Ensure the proper bounds are validated before releasing memory with Scandir

---

HPE ProLiant Agentless Management Service for Windows X64
Version: 10.60.0.0 (C) **(Optional)**
Filename: cp035485.exe

Prerequisites

The *HPE ProLiant iLO 3/4 Channel Interface Driver for Windows X64* (version 3.4.0.0 or later) must be installed prior to this component.

Fixes

Version 10.60.0.0(C) was created to support Windows Server 2012 exclusively. If version 10.60.0 is currently installed on the target platform, then it is not necessary to upgrade to 10.60.0(C).

HPE Smart Storage Administrator (HPE SSA) CLI for Linux 64-bit
Version: 3.30.14.0 **(Recommended)**
Filename: ssacli-3.30-14.0.x86_64.compsig; ssacli-3.30-14.0.x86_64.rpm; ssacli-3.30-14.0.x86_64.txt

Important Note!

It is recommended to update to this 3.30.13.0 version of HPE Smart Storage Administrator if you update your system BIOS using the 2018.06 version of SPP. Any array created with the BIOS configuration utility from the 2018.06 version of SPP will not be accessible with an older version of HPE Smart Storage Administrator.

HPE SSACLI will allow you to configure and manage your storage as before, but now with additional features, abilities, and supported devices. Existing ACUCLI scripts should only need to make minimal changes such as calling the appropriate binary or executable in order to maintain compatibility.

Enhancements

- Added the ability to enable or disable Drive Write Cache for configured and unconfigured drives

---

HPE Smart Storage Administrator (HPE SSA) CLI for VMware 6.0
Version: 3.30.14.0 **(Recommended)**
Filename: ssacli-3.30.14.0-6.0.0.vib

Important Note!

It is recommended to update to this 3.30.13.0 version of HPE Smart Storage Administrator if you update your system BIOS using the 2018.06 version of SPP. Any array created with the BIOS configuration utility from the 2018.06 version of SPP will not be accessible with an older version of HPE Smart Storage Administrator.

Enhancements

- Added the ability to enable or disable Drive Write Cache for configured and unconfigured drives

---

HPE Smart Storage Administrator (HPE SSA) CLI for VMware 6.5
Version: 3.30.14.0 **(Recommended)**
Filename: ssacli-3.30.14.0-6.5.0.vib

Important Note!

It is recommended to update to this 3.30.13.0 version of HPE Smart Storage Administrator if you update your system BIOS using the 2018.06 version of SPP. Any array created with the BIOS configuration utility from the 2018.06 version of SPP will not be accessible with an older version of HPE Smart Storage Administrator.

Enhancements

- Added the ability to enable or disable Drive Write Cache for configured and unconfigured drives

---

HPE Smart Storage Administrator (HPE SSA) CLI for Windows 64-bit
Version: 3.30.14.0 **(Recommended)**
Filename: cp034622.compsig; cp034622.exe

Important Note!

It is recommended to update to this 3.30.13.0 version of HPE Smart Storage Administrator if you update your system BIOS using the 2018.06 version of SPP. Any array created with the BIOS configuration utility from the 2018.06 version of SPP will not be accessible with an older version of HPE Smart Storage Administrator.

HPE SSACLI will allow you to configure and manage your storage as before, but now with additional features, abilities, and supported devices. Existing ACUCLI scripts should only need to make minimal changes such as calling the appropriate binary or executable in order to maintain compatibility.

Enhancements

- Added the ability to enable or disable Drive Write Cache for configured and unconfigured drives

---

HPE Smart Storage Administrator (HPE SSA) for Linux 64-bit
Version: 3.30.14.0 **(Recommended)**
Filename: ssa-3.30-14.0.x86_64.compsig; ssa-3.30-14.0.x86_64.rpm; ssa-3.30-14.0.x86_64.txt

Important Note!

It is recommended to update to this 3.30.13.0 version of HPE Smart Storage Administrator if you update your system BIOS using the 2018.06 version of SPP. Any array created with the BIOS configuration utility from the 2018.06 version of SPP will not be accessible with an older version of HPE Smart Storage Administrator.

HPE SSA replaces the existing HP Array Configuration Utility, or ACU, with an updated design and will deliver new features and functionality for various Smart Storage initiatives as they come online. HPE Smart Array Advanced Pack 1.0 and 2.0 features are now part of the baseline features of HPE SSA, with the appropriate firmware.

HPE SSA will allow you to configure and manage your storage as before, but now with additional features, abilities, and supported devices. Existing ACU scripts should only need to make minimal changes such as calling the appropriate binary or executable in order to maintain compatibility.

Prerequisites

The HPE Smart Storage Administrator for Linux requires the HPE System Management Homepage software to be installed on the server. If the HPE System Management Homepage software is not already installed on your server, please download it from HPE.com and install it before installing the HPE Smart Storage Administrator for Linux.

IMPORTANT UPDATE: HPE SSA (GUI) for Linux can now be run without requiring the HPE System Management Homepage. HPE SSA now supports a Local Application Mode for Linux. The HPE System Management Homepage is still supported, but no longer required to run the HPE SSA GUI.

To invoke, enter the following at the command prompt:

ssa -local

The command will start HP SSA in a new Firefox browser window. When the browser window is closed, HP SSA will automatically stop. This is only valid for the loopback interface, and not visible to external network connections.

Enhancements

- Added the ability to enable or disable Drive Write Cache for configured and unconfigured drives

---

HPE Smart Storage Administrator (HPE SSA) for Windows 64-bit
Version: 3.30.14.0 **(Recommended)**
Filename: cp034621.compsig; cp034621.exe

Important Note!

It is recommended to update to this 3.30.13.0 version of HPE Smart Storage Administrator if you update your system BIOS using the

2018.06 version of SPP. Any array created with the BIOS configuration utility from the 2018.06 version of SPP will not be accessible with an older version of HPE Smart Storage Administrator.

HPE SSA replaces the existing HP Array Configuration Utility, or ACU, with an updated design and will deliver new features and functionality for various Smart Storage initiatives as they come online. HPE Smart Array Advanced Pack 1.0 and 2.0 features are now part of the baseline features of HPE SSA, with the appropriate firmware.

HPE SSA will allow you to configure and manage your storage as before, but now with additional features, abilities, and supported devices. Existing ACU scripts should only need to make minimal changes such as calling the appropriate binary or executable in order to maintain compatibility.

Enhancements

- Added the ability to enable or disable Drive Write Cache for configured and unconfigured drives

---

HPE Smart Storage Administrator Diagnostic Utility (HPE SSADU) CLI for Linux 64-bit
Version: 3.30.14.0 **(Recommended)**
Filename: ssaducli-3.30-14.0.x86_64.compsig; ssaducli-3.30-14.0.x86_64.rpm; ssaducli-3.30-14.0.x86_64.txt

Important Note!

It is recommended to update to this 3.30.13.0 version of HPE Smart Storage Administrator if you update your system BIOS using the 2018.06 version of SPP. Any array created with the BIOS configuration utility from the 2018.06 version of SPP will not be accessible with an older version of HPE Smart Storage Administrator.

This stand alone version of the HPE Smart Storage Administrator's Diagnostic feature is available only in CLI form. For the GUI version of Diagnostic reports, please use HPE Smart Storage Administrator (HPE SSA).

Enhancements

- Added the ability to enable or disable Drive Write Cache for configured and unconfigured drives

---

HPE Smart Storage Administrator Diagnostic Utility (HPE SSADU) CLI for Windows 64-bit
Version: 3.30.14.0 **(Recommended)**
Filename: cp034623.compsig; cp034623.exe

Important Note!

It is recommended to update to this 3.30.13.0 version of HPE Smart Storage Administrator if you update your system BIOS using the 2018.06 version of SPP. Any array created with the BIOS configuration utility from the 2018.06 version of SPP will not be accessible with an older version of HPE Smart Storage Administrator.

This stand alone version of the HPE Smart Storage Administrator's Diagnostic feature is available only in CLI form. For the GUI version of Diagnostic reports, please use HPE Smart Storage Administrator (HPE SSA).

Enhancements

- Added the ability to enable or disable Drive Write Cache for configured and unconfigured drives

---

HPE SNMP Agents for Red Hat Enterprise Linux 6 (AMD64/EM64T)
Version: 10.8.0 **(Optional)**
Filename: hp-snmp-agents-10.80-2965.21.rhel6.x86_64.rpm

Prerequisites

The hp-health and hp-snmp-agents run as 32 bit applications in the x86_64 environment. The Linux kernel 32 bit compatibility must be enabled (usual default for Linux) and the 32 bit compatibility libraries must be present.

To get the list of all dependency files for hp-snmp-agents type:

rpm –qp –-requires hp-snmp-agents-<version>.rpm

Fixes

Fixed the following items:
Enabled additional debugging information for the storage agents debuginfo rpm

---

HPE SNMP Agents for Red Hat Enterprise Linux 7 Server
Version: 10.8.0 **(Optional)**
Filename: hp-snmp-agents-10.80-2965.21.rhel7.x86_64.rpm

Prerequisites

The hp-health and hp-snmp-agents run as 32 bit applications in the x86_64 environment. The Linux kernel 32 bit compatibility must be enabled (usual default for Linux) and the 32 bit compatibility libraries must be present.

To get the list of all dependency files for hp-snmp-agents type:

rpm –qp –-requires hp-snmp-agents-<version>.rpm

Fixes

Fixed the following items:
Enabled additional debugging information for the storage agents debuginfo rpm

---

HPE SNMP Agents for SUSE LINUX Enterprise Server 11 (AMD64/EM64T)
Version: 10.8.0 **(Optional)**
Filename: hp-snmp-agents-10.80-2965.21.sles11.x86_64.rpm

Prerequisites

The hp-health and hp-snmp-agents run as 32 bit applications in the x86_64 environment. The Linux kernel 32 bit compatibility must be enabled (usual default for Linux) and the 32 bit compatibility libraries must be present.

To get the list of all dependency files for hp-snmp-agents type:

rpm –qp –-requires hp-snmp-agents-<version>.rpm

Fixes

Fixed the following items:
Enabled additional debugging information for the storage agents debuginfo rpm

---

HPE SNMP Agents for SUSE LINUX Enterprise Server 12
Version: 10.8.0 **(Optional)**
Filename: hp-snmp-agents-10.80-2965.22.sles12.x86_64.rpm

Prerequisites

The hp-health and hp-snmp-agents run as 32 bit applications in the x86_64 environment. The Linux kernel 32 bit compatibility must be enabled (usual default for Linux) and the 32 bit compatibility libraries must be present.

To get the list of all dependency files for hp-snmp-agents type:

rpm –qp –-requires hp-snmp-agents-<version>.rpm

Fixes

Fixed the following items:
Enabled additional debugging information for the storage agents debuginfo rpm

---

HPE System Health Application and Command Line Utilities for Red Hat Enterprise Linux 6 (AMD64/EM64T)
Version: 10.8.0 **(Optional)**
Filename: hp-health-10.80-1855.27.rhel6.x86_64.rpm

Prerequisites

The hp-health and hp-snmp-agents run as 32 bit applications in the x86_64 environment. The Linux kernel 32 bit compatibility must be enabled (usual default for Linux) and the 32 bit compatibility libraries must be present.

To get the list of all dependency files for hp-health, type:

rpm –qp –requires hp-health-< version >.rpm

Fixes

Fixed the following items:
Add a new constraint to avoid buffer overflow while retrieving device information.

HPE System Health Application and Command Line Utilities for Red Hat Enterprise Linux 7 Server
Version: 10.8.0 **(Optional)**
Filename: hp-health-10.80-1855.21.rhel7.x86_64.rpm

Prerequisites

The hp-health and hp-snmp-agents run as 32 bit applications in the x86_64 environment. The Linux kernel 32 bit compatibility must be enabled (usual default for Linux) and the 32 bit compatibility libraries must be present.

To get the list of all dependency files for hp-health, type:

rpm –qp –requires hp-health-< version >.rpm

Fixes

Fixed the following items:
Add a new constraint to avoid buffer overflow while retrieving device information.

HPE System Health Application and Command Line Utilities for SUSE LINUX Enterprise Server 11 (AMD64/EM64T)
Version: 10.8.0 **(Optional)**
Filename: hp-health-10.80-1855.21.sles11.x86_64.rpm

Prerequisites

The hp-health and hp-snmp-agents run as 32 bit applications in the x86_64 environment. The Linux kernel 32 bit compatibility must be enabled (usual default for Linux) and the 32 bit compatibility libraries must be present.

To get the list of all dependency files for hp-health, type:

rpm –qp –requires hp-health-< version >.rpm

Fixes

Fixed the following items:
Add a new constraint to avoid buffer overflow while retrieving device information.

HPE System Health Application and Command Line Utilities for SUSE LINUX Enterprise Server 12
Version: 10.8.0 **(Optional)**
Filename: hp-health-10.80-1855.22.sles12.x86_64.rpm

Prerequisites

The hp-health and hp-snmp-agents run as 32 bit applications in the x86_64 environment. The Linux kernel 32 bit compatibility must be enabled (usual default for Linux) and the 32 bit compatibility libraries must be present.

To get the list of all dependency files for hp-health, type:

rpm –qp –requires hp-health-< version >.rpm

Fixes

Fixed the following items:
Add a new constraint to avoid buffer overflow while retrieving device information.

HPE System Management Homepage for Linux (AMD64/EM64T)
Version: 7.6.3-3 **(Optional)**
Filename: hpsmh-7.6.3-3.x86_64.rpm

Important Note!

SMH 7.6.0 & later versions, will support only Gen 8 and Gen 9 servers. Any future patch releases could be available, only on SMH web page. Please refer to HPE SMH Release Notes

Precautions for the user on Linux OS:

- Do not provide login access to the "hpsmh" user (created during installation) by editing the /etc/passwd file or any other means
- Do not add any user to the "hpmsh" group (created during installation)

Prerequisites

Before installing the SMH software, the RPM verifies that the required versions of Linux library dependencies are present. If any dependencies are not present, then a list of the missing dependencies is provided. The user must manually install all missing dependencies to satisfy the prerequisites before proceeding with the RPM installation.

Enhancements

Updated the following components:

- PHP to version 5.6.30
- Zlib to version 1.2.11
- PCRE to version 8.41
- Libxslt to version 1.1.32

HPE System Management Homepage for Windows x64
Version: 7.6.3.3 **(Recommended)**
Filename: cp034022.exe

Important Note!

SMH 7.6.0 & later versions, will support only Gen 8 and Gen 9 servers. Any future patch releases could be available, only on SMH web page. Please refer to HPE SMH Release Notes

Enhancements

Updated the following components:

- PHP to version 5.6.30
- Zlib to version 1.2.11
- Libxslt to version 1.1.32
- PCRE to version 8.41

HPE System Management Homepage Templates for Linux
Version: 10.7.0 **(Optional)**
Filename: hp-smh-templates-10.7.0-1485.2.noarch.rpm

Prerequisites

The **hp-smh-templates** RPM install will fail, if all dependencies are not installed. The administrator can verify the list of dependencies required by running this command. If the repositories being used by yum or zypper, includes these dependencies, the installation tool will automatically retrieve them. However if they are not present, the user must manually install them prior to proceeding with the RPM install.

To get the list of all dependency files for hp-smh-templates type:

rpm –qp –-requires hp-smh-templates-<version>.rpm

Fixes

Fixed the following items:

- Corrected the "technology field" at Memory Details page by updating cpqHeResMemModuleTechnology

---

Insight Diagnostics Online Edition for Linux (x86-64)
Version: 10.60.2199 **(Recommended)**
Filename: hpdiags-10.60.2199-2188.linux.x86_64.rpm

Important Note!

The online version of Insight Diagnostics provides the same functionality as the Survey Utility for Windows and Linux and does not perform any hardware tests on the system. Although not required, it is recommended that you uninstall the current Survey Utility for Windows or Linux before beginning the installation of Insight Diagnostics Online Edition.

Prerequisites

The following component(s) are required for Insight Diagnostics Online Edition for Linux:

- System Management Homepage, version 7.0.0-12 or higher

The following component(s) are recommended for Insight Diagnostics Online Edition for Linux to make full use of its capabilities:

- System Health Application, version 9.0.0 or higher

You can install them by using the SPP or downloading them individually from HPE Support Center.

Fixes

- XSS vulnerability in the online page
- libsgutils symlink fix

Enhancements

See the Service Pack for ProLiant Release Notes for more information.

See the Service Pack for ProLiant Server Support Guide for information on supported servers.

Insight Diagnostics Online Edition for Windows x64 Editions
Version: 10.60.2196.0 (A) **(Recommended)**
Filename: cp034727.exe

Important Note!

Known Limitations

1. Under Insight Diagnostics Online Edition for Windows, the Survey feature no longer supports displaying properties of Logical Drives that are attached to certain Smart Array controllers, either directly or through an enclosure (such as an Modular Smart Array). The controllers affected are:

- Smart Array 6i Controller
- Smart Array 641 Controller
- Smart Array 642 Controller
- Smart Array 6402 Controller
- Smart Array 6404 Controller

These controllers do not support the commands used to obtain logical drive properties. There are currently no plans to add such support to the controllers, nor to add legacy support to future versions of Insight Diagnostics.

As a work-around, Insight Diagnostics Online Edition for Windows, version **8.5 or earlier**, may be used to display logical drive properties in Survey. The Array Configuration Utility, available from hpe.com, can also display information about logical drives attached to these controllers.

2. Windows Server 2008 R2 SP1 is the minimum requirement for Gen9 platforms.

3. Adaptec devices are no longer supported on this version, please use version 10.16.1650 for this.

Other:

1. The online version of Insight Diagnostics provides the same functionality as the Survey Utility for Windows and Linux and does not perform any hardware tests on the system. Although not required, it is recommended that you uninstall the current Survey Utility for Windows or Linux before beginning the installation of Insight Diagnostics Online Edition.

Prerequisites

The following component(s) are required for Insight Diagnostics Online Edition for Windows:

- System Management Homepage, version 7.0.0-12 or higher

The following component(s) are recommended for Insight Diagnostics Online Edition for Windows to make full use of its capabilities:

- ProLiant Agentless Management Service, version 9.0.0.0 or higher
- ProLiant Integrated Lights-Out Management Interface Driver, version 1.15.0.0 or higher

Enhancements

Addded support for P542D storage controller.
Added support for NVIDIA Tesla K40 XL 12Gb Module.
Support Wellsburg 6-Port SATA Controller.
Support for new Gen9 systems.

See the Service Pack for ProLiant Release Notes for more information.

See the Service Pack for ProLiant Server Support Guide for information on supported servers.

Integrated Management Log Viewer for Windows Server x64 Editions
Version: 7.8.0.0 **(Optional)**
Filename: cp029435.exe

Important Note!

Starting with version 7.0.0.0, this application will only install on HP ProLiant systems supporting the iLO 2, iLO 3, or iLO 4 management controllers. Installation in a virtual machine is no longer supported.

Starting with version 6.5.0.0, this application requires Administrator privileges through Windows User Account Control.

Version 6.2.0.0 of this application is the final version that will support installation under Windows Server 2003 x64 Edition.

Starting with version 6.0.0.0, the dependencies on the HP ProLiant Remote Monitor Service and the HP ProLiant Remote IML Service have

been removed. This application no longer provides access to the Integrated Management Log on a remote system.

Starting with version 5.22.0.0, separate 32-bit and 64-bit releases of this application are available. If you wish to downgrade to version 5.21.0.0 or earlier, use Windows Add or Remove Programs to uninstall the 64-bit release before installing the earlier 32-bit version.

Enhancements

Add support for Windows Server 2016.

NVMe Drive Eject NMI Fix for Intel Xeon Processor Scalable Family for Windows
Version: 1.1.0.0 (B) **(Optional)**
Filename: cp033116.compsig; cp033116.exe

Enhancements

Enabled deployment to iLO 5 nodes when used with Smart Update Manager version 8.2.0 or later.

NVMe Drive Eject NMI Fix for Intel Xeon v3 and Xeon v4 Processors for Windows Server 2012 R2 and Server 2016
Version: 1.0.5.0 (B) **(Optional)**
Filename: cp030432.exe

Enhancements

Changed component name to indicate which processors are supported. Systems that already have version 1.0.5.0 installed do not need to install this component.
