Service Pack for ProLiant, v2018.09.0コンポーネントリリースノート

BIOS - システムROM

先頭

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant DL380 Gen9/DL360 Gen9(P89) サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-p89-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL360/DL380 Gen9 システムROM - P89

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイク

ロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant DL380 Gen9/DL360 Gen9(P89)サーバー

バージョン: 2.60_05-21-2018 (B) **(クリティカル)**
ファイル名: cp037244.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

バージョン2.60_05-21-2018 (B)にはコンポーネントパッケージのアップデートが含まれており、機能的にはバージョン2.60_05-21-2018と同等です。 ファームウェアをバージョン2.60_05-21-2018にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョン(B)にアップグレードする必要はありません。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステム

では、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL360/DL380 Gen9 システムROM - P89

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

バージョン2.60_05-21-2018 (B)にはコンポーネントパッケージのアップデートが含まれており、機能的にはバージョン2.60_05-21-2018と同等です。 ファームウェアをバージョン2.60_05-21-2018にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョン(B)にアップグレードする必要はありません。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

Linux用オンラインROMフラッシュコンポーネント - HPE Synergy 480 Gen10(I42)コンピュートモジュール

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: RPMS/x86_64/firmware-system-i42-1.42_2018_06_20-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-i42-1.42_2018_06_20-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 480 Gen10コンピュートモジュールシステムROM - I42

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

Linux用オンラインROMフラッシュコンポーネント - HPE Synergy 480 Gen9 (I37) コンピュートモジュール

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-i37-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 480 Gen9 System ROM - I37

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

Linux用オンラインROMフラッシュコンポーネント - HPE Synergy 660 Gen10(I43)コンピュートモジュール

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: RPMS/x86_64/firmware-system-i43-1.42_2018_06_20-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-i43-1.42_2018_06_20-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 660 Gen10コンピュートモジュールシステムROM - I43

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

Linux用オンラインROMフラッシュコンポーネント - HPE Synergy 660 Gen9 (I39) コンピュートモジュール

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-i39-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 660 Gen9 System ROM - I39

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant DL580 Gen9 (U17) Servers

バージョン: 2.60_05-23-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u17-2.60_2018_05_23-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL580 Gen9 システムROM - U17

リリースバージョン:

2.60_05-23-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-23-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant XL270d Gen10 (U45) Servers

バージョン: 1.42_06-20-2018 **(クリティカル)**

ファイル名: RPMS/x86_64/firmware-system-u45-1.42_2018_06_20-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u45-1.42_2018_06_20-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL270d Gen10システムROM - U45

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステム

では、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant DL580 Gen9 (U17) Servers

バージョン: 2.60_05-23-2018 **(クリティカル)**
ファイル名: CP035892.compsig; CP035892.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正

に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL580 Gen9 システムROM - U17

リリースバージョン:

2.60_05-23-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-23-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。

1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。

ESXi 5.5、ESXi 6.0、およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。

2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。

ESXi 5.5の最小CRUバージョンは5.5.4.1です。

ESXi 6.0の最小CRUバージョンは6.0.8です。

6.5の最小CRUバージョンは6.5.8です。

6.7の最小CRUバージョンは6.7.10です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、および5.5用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant DL160 Gen9/DL180 Gen9 (U20) Servers

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035854.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステム

では、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL160/DL180 Gen9 システムROM - U20

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれ

ています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant DL580 Gen9 (U17) Servers

バージョン: 2.60_05-23-2018 **(クリティカル)**
ファイル名: cp035893.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL580 Gen9 システムROM - U17

リリースバージョン:

2.60_05-23-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-23-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

ROM Flash Firmware Package - HPE Apollo 2000 Gen10/HPE ProLiant XL170r/XL190r Gen10 (U38) Servers

バージョン: 1.42_06-23-2018 **(クリティカル)**
ファイル名: U38_1.42_06_23_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL170r/XL190r Gen10 システムROM - U38

リリースバージョン:

1.42_06-23-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-23-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

ROM Flash Firmware Package - HPE Apollo 4510 Gen10/HPE ProLiant XL450 Gen10 (U40) Servers

バージョン: 1.42_06-23-2018 **(クリティカル)**
ファイル名: U40_1.42_06_23_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL450 Gen10 システムROM - U40

リリースバージョン:

1.42_06-23-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-23-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

ROM Flash Firmware Package - HPE ProLiant BL460c Gen10 (I41) Servers

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: I41_1.42_06_20_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant BL460c Gen10システムROM - I41

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

ROM Flash Firmware Package - HPE ProLiant DL560 Gen10/DL580 Gen10 (U34) Servers

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: U34_1.42_06_20_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL560/DL580 Gen10システムROM - U34

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

ROM Flash Firmware Package - HPE ProLiant ML110 Gen10 (U33) Servers

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: U33_1.42_06_20_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML110 Gen10システムROM - U33

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャ

ッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

ROM Flash Firmware Package - HPE ProLiant ML350 Gen10 (U41) Servers

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: U41_1.42_06_20_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML350 Gen10システムROM - U41

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

ROM Flash Firmware Package - HPE ProLiant XL230k Gen10 (U37) Server

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: U37_1.42_06_20_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL230k Gen10システムROM - U37

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

ROM Flash Firmware Package - HPE Synergy 480 Gen10 (I42) Compute Module

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: I42_1.42_06_20_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステム

では、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 480 Gen10コンピュートモジュールシステムROM - I42

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDは

CVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

ROM Flash Firmware Package - HPE Synergy 660 Gen10 (I43) Compute Module

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: I43_1.42_06_20_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 660 Gen10コンピュートモジュールシステムROM - I43

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

ROMフラッシュファームウェアパッケージ - HPE ProLiant DL360 Gen10(U32)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: U32_1.42_06_20_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL360 Gen10システムROM - U32

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

ROMフラッシュファームウェアパッケージ - HPE ProLiant DL380 Gen10(U30)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: U30_1.42_06_20_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL380 Gen10システムROM - U30

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバー

に固有のものではありません。

NVDIMM-NメモリまたはScalable Persistent Memoryで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-NメモリまたはScalable Persistent Memoryで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

ROMフラッシュファームウェアパッケージ - HPE ProLiant XL270d Gen10(U45)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: U45_1.42_06_20_2018.fwpkg

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL270d Gen10システムROM - U45

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステム

では、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

VMware用オンラインROMフラッシュコンポーネント - HPE Synergy 480 Gen9 (I37) コンピュートモジュール

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035855.compsig; CP035855.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 480 Gen9 System ROM - I37

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイク

ロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。
ESXi 5.5、ESXi 6.0、ESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。

6.7の最小CRUバージョンは6.7.10です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、および5.5用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

VMware用オンラインROMフラッシュコンポーネント - HPE Synergy 660 Gen9 (I39) コンピュートモジュール

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035828.compsig; CP035828.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 660 Gen9 System ROM - I39

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。
ESXi 5.5、ESXi 6.0、ESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。

6.7の最小CRUバージョンは6.7.10です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、および5.5用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されて

しまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

Windows x64用オンラインROMフラッシュコンポーネント - HPE Synergy 480 Gen10(I42)コンピュートモジュール

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: cp036757.compsig; cp036757.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 480 Gen10コンピュートモジュールシステムROM - I42

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

Windows x64用オンラインROMフラッシュコンポーネント - HPE Synergy 480 Gen9 (I37) コンピュートモジュール

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035852.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 480 Gen9 System ROM - I37

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

Windows x64用オンラインROMフラッシュコンポーネント - HPE Synergy 620/680 Gen9 (I40) コンピュートモジュール

バージョン: 2.60_05-23-2018 **(クリティカル)**
ファイル名: cp036454.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在する情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 620 Gen9/680 Gen9 システムROM - I40

リリースバージョン:

2.60_05-23-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-23-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在する情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI (Quick Path Interlink) エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在する情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在する情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしま

う可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI (Quick Path Interlink) エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

Windows x64用オンラインROMフラッシュコンポーネント - HPE Synergy 660 Gen10(I43)コンピュートモジュール

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: cp036759.compsig; cp036759.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 660 Gen10コンピュートモジュールシステムROM - I43

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバー

に固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

Windows x64用オンラインROMフラッシュコンポーネント - HPE Synergy 660 Gen9 (I39) コンピュートモジュール

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035829.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 660 Gen9 System ROM - I39

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE Apollo 2000 Gen10/HPE ProLiant XL170r/XL190r Gen10 (U38) サーバー

バージョン: 1.42_06-23-2018 **(クリティカル)**
ファイル名: cp036761.compsig; cp036761.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL170r/XL190r Gen10 システムROM - U38

リリースバージョン:

1.42_06-23-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-23-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

オンラインROMフラッシュコンポーネント for Windows x64 - HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9 (U19) サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035944.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9システムROM - U19

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE Apollo 4510 Gen10/HPE ProLiant XL450 Gen10 (U40) サーバー

バージョン: 1.42_06-23-2018 **(クリティカル)**
ファイル名: cp036790.compsig; cp036790.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL450 Gen10 システムROM - U40

リリースバージョン:

1.42_06-23-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-23-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant BL460c Gen9/WS460c Gen9(I36)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-i36-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれ

ています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant BL460c Gen9/WS460c Gen9 システムROM - I36

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant BL660c Gen9(I38)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-i38-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant BL660c Gen9 システムROM - I38

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイク

ロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant DL160 Gen9/DL180 Gen9(U20) サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u20-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL160/DL180 Gen9 システムROM - U20

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant DL325 Gen10 (A41)サーバー

バージョン: 1.30_06-07-2018 **(推奨)**
ファイル名: RPMS/x86_64/firmware-system-a41-1.30_2018_06_07-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-a41-1.30_2018_06_07-1.1.x86_64.rpm

重要な注意！

重要な注意:

なし

提供名:

HPE ProLiant DL325 Gen10システムROM - A41

リリースバージョン:

1.30_06-07-2018

最新の推奨またはクリティカルリビジョン:

これは、このファームウェアでの最初のバージョンです。

以前のリビジョン:

これは、このファームウェアでの最初のバージョンです。

ファームウェアの依存関係:

なし

改善点/新しい機能:

これは、このファームウェアでの最初のバージョンです。

修正された問題点:

なし

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

拡張

重要な注意:

なし

ファームウェアの依存関係:

なし

改善点/新しい機能:

これは、このファームウェアでの最初のバージョンです。

既知の問題点:

なし

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant DL380 Gen10(U30)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: RPMS/x86_64/firmware-system-u30-1.42_2018_06_20-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u30-1.42_2018_06_20-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行う

システムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL380 Gen10システムROM - U30

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-NメモリまたはScalable Persistent Memoryで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-NメモリまたはScalable Persistent Memoryで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant DL560 Gen10/DL580 Gen10(U34)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: RPMS/x86_64/firmware-system-u34-1.42_2018_06_20-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u34-1.42_2018_06_20-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL560/DL580 Gen10システムROM - U34

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

拡張

なし

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant DL560 Gen9(P85)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-p85-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL560 Gen9 システムROM - P85

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステム

では、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant DL60 Gen9/DL80 Gen9(U15)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u15-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意事項:このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL60/DL80 Gen9 システムROM - U15

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行う

システムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant ML110 Gen9(P99)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-p99-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML110 Gen9 システムROM - P99

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant ML150 Gen9(P95)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-p95-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャ

ッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML150 Gen9 システムROM - P95

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant ML350 Gen9(P92)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-p92-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML350 Gen9 システムROM - P92

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行う

システムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant XL230a/XL250a Gen9(U13)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u13-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL230a/XL250a Gen9 システムROM - U13

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイク

ロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant XL230k Gen10 (U37)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: RPMS/x86_64/firmware-system-u37-1.42_2018_06_20-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u37-1.42_2018_06_20-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL230k Gen10システムROM - U37

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

拡張

なし

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant XL260a Gen9/XL2x260w (U24) サーバー

バージョン: 1.60_01-22-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u24-1.60_2018_01_22-1.1.i386.rpm

重要な注意！

重要な注意:

このリビジョンのシステムROMにはインテルのマイクロコードの最新リビジョンが含まれており、オペレーティングシステムのアップデートとの組み合わせで、サイドチャネル解析の脆弱性のバリアント2(Spectreとも呼ばれます)を緩和します。このシステムROMに含まれているマイクロコードのリビジョンでは、Spectreバリアント2の緩和策の一部であった以前のインテルマイクロコードに影響を及ぼしていた、リブート頻度の増加および予測不能なシステム動作の問題はありません。追加情報については、インテルのSecurity Exploit Newsroom(https://newsroom.intel.com/press-kits/security-exploits-intel-products/)から入手できます。

提供名:

HPE ProLiant XL260a Gen9/XL2x260wシステムROM - U24

リリースバージョン:

1.60_01-22-2018

最新の推奨またはクリティカルリビジョン:

1.60_01-22-2018

以前のリビジョン:

1.50_09-25-2017

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

インテルプロセッサーのマイクロコードを最新バージョンにアップデート。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

なし

ファームウェアの依存関係:

なし

修正された問題点:

内蔵メモリ(MCDRAM)をキャッシュモードまたはハイブリッドメモリモードで構成するとシステムで予測不能なシステム動作が発生することがあるという問題に対処しました。この問題は、フラットメモリモードで構成されたシステムには影響しません。この問題は、Hewlett Packard Enterpriseシステムに固有のものではありません。

既知の問題点:

なし

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant XL450 Gen9(U21)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u21-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL450 Gen9 システムROM - U21

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではあり

ません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Linux - HPE ProLiant XL730f/XL740f/XL750f Gen9(U18)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u18-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL730f/XL740f/XL750f Gen9 システムROM - U18

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9 (U19)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035946.compsig; CP035946.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9システムROM - U19

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。
ESXi 5.1、ESXi 5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.1の最小CRUバージョンは5.0.3.9です。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。
6.7の最小CRUバージョンは6.7.10です。
両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ド

ライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant BL460c Gen9/WS460c Gen9 (I36) サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035849.zip

重要な注意！

重要な注意:

このリビジョンのシステムROMにはインテルのマイクロコードの最新リビジョンが含まれており、オペレーティングシステムのアップデートとの組み合わせで、Speculative Store Bypass(Variant 4とも呼ばれます)というセキュリティ上の脆弱性を緩和します。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このリビジョンのシステムROMにはインテルのマイクロコードの最新リビジョンが含まれており、Rogue Register Read(Variant 3aとも呼ばれます)というセキュリティ上の脆弱性を緩和します。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

配布名:

HPE ProLiant BL460c Gen9/WS460c Gen9 システムROM - I36

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このリビジョンのシステムROMにはインテルのマイクロコードの最新リビジョンが含まれており、オペレーティングシステムのアップデートとの組み合わせで、Speculative Store Bypass(Variant 4とも呼ばれます)というセキュリティ上の脆弱性を緩和します。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このリビジョンのシステムROMにはインテルのマイクロコードの最新リビジョンが含まれており、Rogue Register Read(Variant 3aとも呼ばれます)というセキュリティ上の脆弱性を緩和します。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI (Quick Path Interlink) エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。
ESXi 5.1、ESXi 5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.1の最小CRUバージョンは5.0.3.9です。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。
6.7の最小CRUバージョンは6.7.10です。
両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このリビジョンのシステムROMにはインテルのマイクロコードの最新リビジョンが含まれており、オペレーティングシステムのアップデートとの組み合わせで、Speculative Store Bypass(Variant 4とも呼ばれます)というセキュリティ上の脆弱性を緩和します。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このリビジョンのシステムROMにはインテルのマイクロコードの最新リビジョンが含まれており、Rogue Register Read(Variant 3aとも呼ばれます)というセキュリティ上の脆弱性を緩和します。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このリビジョンのシステムROMにはインテルのマイクロコードの最新リビジョンが含まれており、オペレーティングシステムのアップデートとの組み合わせで、Speculative Store Bypass(Variant 4とも呼ばれます)というセキュリティ上の脆弱性を緩和します。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このリビジョンのシステムROMにはインテルのマイクロコードの最新リビジョンが含まれており、Rogue Register Read(Variant 3aとも呼ばれます)というセキュリティ上の脆弱性を緩和します。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI (Quick Path Interlink) エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant BL660c Gen9(I38)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**

ファイル名: CP035823.compsig; CP035823.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant BL660c Gen9 システムROM - I38

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。
ESXi 5.1、ESXi 5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.1の最小CRUバージョンは5.0.3.9です。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。
6.7の最小CRUバージョンは6.7.10です。
両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant DL120 Gen9(P86)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035874.compsig; CP035874.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL120 Gen9 システムROM - P86

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。

1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。

ESXi 5.1、5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。

2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。

ESXi 5.1の最小CRUバージョンは5.0.3.9です。

ESXi 5.5の最小CRUバージョンは5.5.4.1です。

ESXi 6.0の最小CRUバージョンは6.0.8です。

6.5の最小CRUバージョンは6.5.8です。

6.7の最小CRUバージョンは6.7.10です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではあり

ません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant DL160 Gen9/DL180 Gen9 (U20) サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035857.compsig; CP035857.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL160/DL180 Gen9 システムROM - U20

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。

1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。

ESXi 5.1、ESXi 5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。

2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。

5.1の最小CRUバージョンは5.0.3.9です。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。
6.7の最小CRUバージョンは6.7.10です。
両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant DL380 Gen9/DL360 Gen9(P89)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035814.compsig; CP035814.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL360/DL380 Gen9 システムROM - P89

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。

1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。

ESXi 5.1、5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。

2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。

ESXi 5.1の最小CRUバージョンは5.0.3.9です。

ESXi 5.5の最小CRUバージョンは5.5.4.1です。

ESXi 6.0の最小CRUバージョンは6.0.8です。

6.5の最小CRUバージョンは6.5.8です。

6.7の最小CRUバージョンは6.7.10です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant DL560 Gen9(P85)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035899.compsig; CP035899.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL560 Gen9 システムROM - P85

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。
ESXi 5.1、ESXi 5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.1の最小CRUバージョンは5.0.3.9です。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。
6.7の最小CRUバージョンは6.7.10です。
両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant DL60 Gen9/DL80 Gen9(U15) サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035902.compsig; CP035902.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャ

ッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL60/DL80 Gen9 システムROM - U15

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。

1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。

ESXi 5.1、5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。

2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。

ESXi 5.1の最小CRUバージョンは5.0.3.9です。

ESXi 5.5の最小CRUバージョンは5.5.4.1です。

ESXi 6.0の最小CRUバージョンは6.0.8です。

6.5の最小CRUバージョンは6.5.8です。

6.7の最小CRUバージョンは6.7.10です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイク

ロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant ML110 Gen9(P99)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035851.compsig; CP035851.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML110 Gen9 システムROM - P99

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。
ESXi 5.1、ESXi 5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.1の最小CRUバージョンは5.0.3.9です。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。
6.7の最小CRUバージョンは6.7.10です。
両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャ

ッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant ML150 Gen9(P95)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035878.compsig; CP035878.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML150 Gen9 システムROM - P95

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。
ESXi 5.1、ESXi 5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.1の最小CRUバージョンは5.0.3.9です。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。
6.7の最小CRUバージョンは6.7.10です。
両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant ML350 Gen9(P92)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035961.compsig; CP035961.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML350 Gen9 システムROM - P92

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。
ESXi 5.1、ESXi 5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.1の最小CRUバージョンは5.0.3.9です。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。

6.5の最小CRUバージョンは6.5.8です。
6.7の最小CRUバージョンは6.7.10です。
両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware - HPE ProLiant XL450 Gen9(U21)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035821.compsig; CP035821.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL450 Gen9 システムROM - U21

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。

1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要がありま

す。
ESXi 5.1、ESXi 5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.1の最小CRUバージョンは5.0.3.9です。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。
6.7の最小CRUバージョンは6.7.10です。
両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for VMware ESXi - HPE ProLiant XL230a/XL250a Gen9(U13)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035826.compsig; CP035826.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL230a/XL250a Gen9 システムROM - U13

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。
ESXi 5.1、ESXi 5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.1の最小CRUバージョンは5.0.3.9です。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。
6.7の最小CRUバージョンは6.7.10です。
両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant BL460c Gen9/WS460c Gen9 (I36)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035846.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant BL460c Gen9/WS460c Gen9 システムROM - I36

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれ

ています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant BL660c Gen9 (I38)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035824.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant BL660c Gen9 システムROM - I38

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant DL380 Gen10 (U30)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: cp036824.compsig; cp036824.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDは

CVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL380 Gen10システムROM - U30

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-NメモリまたはScalable Persistent Memoryで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-NメモリまたはScalable Persistent Memoryで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant DL560 Gen10/DL580 Gen10 (U34)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: cp036780.compsig; cp036780.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL560/DL580 Gen10システムROM - U34

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant DL560 Gen9 (P85)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035897.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL560 Gen9 システムROM - P85

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant DL60 Gen9/DL80 Gen9(U15)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035903.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL60/DL80 Gen9 システムROM - U15

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、ID

はCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。 投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant ML110 Gen9 (P99)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035847.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML110 Gen9 システムROM - P99

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant ML150 Gen9 (P95)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035876.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML150 Gen9 システムROM - P95

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant ML350 Gen9(P92)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035797.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML350 Gen9 システムROM - P92

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant XL170r/XL190r Gen9(U14)サーバー

バージョン: 2.60_05-22-2018 **(クリティカル)**
ファイル名: cp035890.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL170r/190r Gen9 システムROM - U14

リリースバージョン:

2.60_05-22-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-22-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャ

ッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant XL230a/XL250a Gen9 (U13)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035811.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL230a/XL250a Gen9 システムROM - U13

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行う

システムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant XL230k Gen10 (U37)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: cp036766.compsig; cp036766.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれ

ています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL230k Gen10システムROM - U37

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

拡張

なし

オンラインROMフラッシュコンポーネント for Windows x64 - HPE ProLiant XL450 Gen9 (U21)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035810.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL450 Gen9 システムROM - U21

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor Linux - HPE Apollo 2000 Gen10/HPE ProLiant XL170r/XL190r Gen10 (U38) サーバー

バージョン: 1.42_06-23-2018 **(クリティカル)**
ファイル名: RPMS/x86_64/firmware-system-u38-1.42_2018_06_23-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u38-1.42_2018_06_23-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL170r/XL190r Gen10 システムROM - U38

リリースバージョン:

1.42_06-23-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-23-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

オンラインROMフラッシュコンポーネントfor Linux - HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9 (U19) サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u19-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Apollo 4200 Gen9/HPE ProLiant XL420 Gen9システムROM - U19

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステム

では、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor Linux - HPE Apollo 4510 Gen10/HPE ProLiant XL450 Gen10 (U40) サーバー

バージョン: 1.42_06-23-2018 **(クリティカル)**
ファイル名: RPMS/x86_64/firmware-system-u40-1.42_2018_06_23-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u40-1.42_2018_06_23-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL450 Gen10 システムROM - U40

リリースバージョン:

1.42_06-23-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-23-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されて

しまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

システムでサーバーの再起動時にSmartストレージバッテリ障害が正しく報告されないことがあるきわめてまれな問題に対処しました。

既知の問題点:

なし

オンラインROMフラッシュコンポーネントfor Linux - HPE ProLiant BL460c Gen10 (I41)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: RPMS/x86_64/firmware-system-i41-1.42_2018_06_20-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-i41-1.42_2018_06_20-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant BL460c Gen10システムROM - I41

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

拡張

なし

オンラインROMフラッシュコンポーネントfor Linux - HPE ProLiant DL120 Gen9(P86)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-p86-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL120 Gen9 システムROM - P86

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイク

ロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor Linux - HPE ProLiant DL20 Gen9 (U22)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u22-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDは

CVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL20 Gen9 システムROM - U22

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

オンラインROMフラッシュコンポーネントfor Linux - HPE ProLiant DL360 Gen10 (U32)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**

ファイル名: RPMS/x86_64/firmware-system-u32-1.42_2018_06_20-1.1.x86_64.compsig; RPMS/x86_64/firmware-

system-u32-1.42_2018_06_20-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL360 Gen10システムROM - U32

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれ

ています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

オンラインROMフラッシュコンポーネントfor Linux - HPE ProLiant DL385 Gen10 (A40) サーバー

バージョン: 1.30_06-07-2018 **(推奨)**
ファイル名: 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

重要な注意！

重要な注意:

なし

配布名:

HPE ProLiant DL385 Gen10システムROM - A40

リリースバージョン:

1.30_06-07-2018

最新の推奨またはクリティカルリビジョン:

1.30_06-07-2018

以前のリビジョン:

1.22_04-16-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

最新のVMware vSphereセキュアブート証明書のサポートを追加しました。

BIOS/プラットフォーム構成(RBSU)の新しいメモリコントローラーインターリーブメニューを追加しました。このオプションでは、不均衡なメモリ構成で構成されたシステムのメモリパフォーマンスを向上させることができるメモリコントローラーインターリーブを無効にできます。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

システムユーティリティのための言語翻訳(英語以外のモード)をアップデートしました。

修正された問題点:

1TB以上のメモリが取り付けられたシステムにメモリリソースが正しく割り当てられていないため、カーネルパニックが発生したりIOMMUでエラーが報告されたりすることがある問題に対処しました。

UEFI POST検出モードオプションが高速検出の強制に設定されている場合に内蔵Diagnosticsが正しく起動しないことがある問題に対処しました。

システムユーティリティメニューのインテグレーテッドマネジメントログ (IML) ビューアーが起動時に応答しなくなることがある問題に対処しました。

UEFI POST検出モードオプションが高速検出の強制に設定されている場合にHPEデュアルSDカードUSBモジュールが正しく起動しないことがある問題に対処しました。

Trusted Platform Module (TPM) がTPM 2.0モード用に構成されている場合にTPMのファームウェアアップデートが正しく完了しないことがある問題に対処しました。この問題は、TPM 1.2モードで動作するTPMで構成されているシステムには影響しません。

サードパーティのUSBキーがサーバーのUSBポートのいずれかに取り付けられている場合にシステムでIntelligent Provisioningを起動できないことがある問題に対処しました。この問題は特定のUSBキーで検出されたものであり、他のデバイスでは検出されていません。

UEFI POST検出モードオプションが完全検出の強制に設定されている場合にIntegrated Lights-Out (iLO) 仮想メディアが正しく起動しないことがある問題に対処しました。

レガシーブートモードで構成されている場合に、BIOS/プラットフォーム構成(RBSU)から無効にされた内蔵SDカードと、取り付けられているHPEデュアルSDカードで構成されたシステムがHPEデュアルSDカードUSBモジュールから起動しない問題に対処しました。この問題は、UEFIブートモードで構成されているシステムには影響しません。

レガシーブートモードで構成されている場合に、オプションのHPE CN1200E-Tアダプターで構成されたシステムが正しく起動しない問題に対処しました。この問題は、UEFIブートモードで構成されているシステムには影響しません。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

なし

ファームウェアの依存関係:

なし

修正された問題点:

1TB以上のメモリが取り付けられたシステムにメモリリソースが正しく割り当てられていないため、カーネルパニックが発生したりIOMMUでエラーが報告されたりすることがある問題に対処しました。

UEFI POST検出モードオプションが高速検出の強制に設定されている場合に内蔵Diagnosticsが正しく起動しないことがある問題に対処しました。

システムユーティリティメニューのインテグレーテッドマネジメントログ (IML) ビューアーが起動時に応答しなくなることがある問題に対処しました。

UEFI POST検出モードオプションが高速検出の強制に設定されている場合にHPEデュアルSDカードUSBモジュールが正しく起動しないことがある問題に対処しました。

Trusted Platform Module (TPM) がTPM 2.0モード用に構成されている場合にTPMのファームウェアアップデートが正しく完了しないことがある問題に対処しました。この問題は、TPM 1.2モードで動作するTPMで構成されているシステムには影響しません。

サードパーティのUSBキーがサーバーのUSBポートのいずれかに取り付けられている場合にシステムでIntelligent Provisioningを起動できないことがある問題に対処しました。この問題は特定のUSBキーで検出されたものであり、他のデバイスでは検出されていません。

UEFI POST検出モードオプションが完全検出の強制に設定されている場合にIntegrated Lights-Out (iLO) 仮想メディアが正しく起動しないことがある問題に対処しました。

レガシーブートモードで構成されている場合に、BIOS/プラットフォーム構成(RBSU)から無効にされた内蔵SDカードと、取り付けられているHPEデュアルSDカードで構成されたシステムがHPEデュアルSDカードUSBモジュールから起動しない問題に対処しました。この問題は、UEFIブートモードで構成されているシステムには影響しません。

レガシーブートモードで構成されている場合に、オプションのHPE CN1200E-Tアダプターで構成されたシステムが正しく起動しない問題に対処しました。この問題は、UEFIブートモードで構成されているシステムには影響しません。

既知の問題点:

なし

拡張

最新のVMware vSphereセキュアブート証明書のサポートを追加しました。

BIOS/プラットフォーム構成(RBSU)の新しいメモリコントローラーインターリーブメニューを追加しました。このオプションでは、不均衡なメモリ構成で構成されたシステムのメモリパフォーマンスを向上させることができるメモリコントローラーインターリーブを無効にできます。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

システムユーティリティのための言語翻訳(英語以外のモード)をアップデートしました。

オンラインROMフラッシュコンポーネントfor Linux - HPE ProLiant EC200a (U26) サーバー/HPE ProLiant Thin Micro TM200 (U26) サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u26-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant Thin Micro TM200サーバーGen9システムROM - U26

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイク

ロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

拡張

なし

オンラインROMフラッシュコンポーネントfor Linux - HPE ProLiant ML110 Gen10 (U33)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: RPMS/x86_64/firmware-system-u33-1.42_2018_06_20-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u33-1.42_2018_06_20-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML110 Gen10システムROM - U33

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

拡張

なし

オンラインROMフラッシュコンポーネントfor Linux - HPE ProLiant ML30 Gen9 (U23)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u23-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML30 Gen9 システムROM - U23

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor Linux - HPE ProLiant ML350 Gen10 (U41) サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: RPMS/x86_64/firmware-system-u41-1.42_2018_06_20-1.1.x86_64.compsig; RPMS/x86_64/firmware-system-u41-1.42_2018_06_20-1.1.x86_64.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイク

ロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML350 Gen10システムROM - U41

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

標準のLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

オンラインROMフラッシュコンポーネントfor Linux - HPE ProLiant XL170r/XL190r Gen9(U14)サーバー

バージョン: 2.60_05-22-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u14-2.60_2018_05_22-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL170r/190r Gen9 システムROM - U14

リリースバージョン:

2.60_05-22-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-22-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor Linux - HPE ProLiant XL270d (U25) アクセラレータトレイ

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-u25-2.60_2018_05_21-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL270dアクセラレータトレイシステムROM - U25

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor Linux - HPE Synergy 620/680 Gen9 (I40) コンピュートモジュール

バージョン: 2.60_05-23-2018 **(クリティカル)**
ファイル名: RPMS/i386/firmware-system-i40-2.60_2018_05_23-1.1.i386.rpm

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 620 Gen9/680 Gen9 システムROM - I40

リリースバージョン:

2.60_05-23-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-23-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前

のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor VMware - HPE ProLiant DL20 Gen9 (U22)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP036398.compsig; CP036398.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL20 Gen9 システムROM - U22

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイク

ロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) をインストールされて稼動している必要があります。
ESXi 5.5、ESXi 6.0、ESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。

6.7の最小CRUバージョンは6.7.10です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、および5.5用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

オンラインROMフラッシュコンポーネントfor VMware - HPE ProLiant EC200a (U26) サーバー/HPE ProLiant Thin Micro TM200 (U26) サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP036461.compsig; CP036461.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開

示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant Thin Micro TM200サーバーGen9システムROM - U26

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。

1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) をインストールされて稼動している必要があります。

ESXi 5.5、ESXi 6.0、およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。

2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。

ESXi 5.5の最小CRUバージョンは5.5.4.1です。

ESXi 6.0の最小CRUバージョンは6.0.8です。

6.5の最小CRUバージョンは6.5.8です。

6.7の最小CRUバージョンは6.7.10です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、および5.5用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDは

CVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

拡張

なし

オンラインROMフラッシュコンポーネントfor VMware - HPE ProLiant ML30 Gen9 (U23)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: CP035706.compsig; CP035706.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML30 Gen9 システムROM - U23

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。
ESXi 5.5、ESXi 6.0、ESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。

6.7の最小CRUバージョンは6.7.10です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、および5.5用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor VMware - HPE ProLiant XL170r/XL190r Gen9 (U14)サーバー

バージョン: 2.60_05-22-2018 **(クリティカル)**
ファイル名: CP035888.compsig; CP035888.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL170r/190r Gen9 システムROM - U14

リリースバージョン:

2.60_05-22-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-22-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。

1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) がインストールおよび実行されている必要があります。

ESXi 5.1、5.5、ESXi 6.0およびESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。

2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。

ESXi 5.1の最小CRUバージョンは5.0.3.9です。

ESXi 5.5の最小CRUバージョンは5.5.4.1です。

ESXi 6.0の最小CRUバージョンは6.0.8です。

6.5の最小CRUバージョンは6.5.8です。

6.7の最小CRUバージョンは6.7.10です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor VMware - HPE Synergy 620/680 Gen9 (I40) コンピュートモジュール

バージョン: 2.60_05-23-2018 **(クリティカル)**
ファイル名: CP036456.compsig; CP036456.zip

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE Synergy 620 Gen9/680 Gen9 システムROM - I40

リリースバージョン:

2.60_05-23-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-23-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。
1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) をインストールされて稼動している必要があります。
ESXi 5.5、ESXi 6.0、ESXi 6.5の最小iLOバージョンは1.4です。 ESXi 6.7の最小iLOバージョンは10.1.0です。
2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。
5.5の最小CRUバージョンは5.5.4.1です。
6.0の最小CRUバージョンは6.0.8です。
6.5の最小CRUバージョンは6.5.8です。

6.7の最小CRUバージョンは6.7.10です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.7、6.5、6.0、および5.5用のOS固有の"HPE Agentless

Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant BL460c Gen10 (I41)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: cp036778.compsig; cp036778.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant BL460c Gen10システムROM - I41

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されて

しまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

拡張

なし

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant DL120 Gen9 (P86)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035875.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL120 Gen9 システムROM - P86

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイク

ロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant DL20 Gen9 (U22)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp036396.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL20 Gen9 システムROM - U22

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性

の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant DL325 Gen10 (A41) サーバー

バージョン: 1.30_06-07-2018 **(推奨)**
ファイル名: cp036636.compsig; cp036636.exe

重要な注意！

重要な注意:

なし

提供名:

HPE ProLiant DL325 Gen10システムROM - A41

リリースバージョン:

1.30_06-07-2018

最新の推奨またはクリティカルリビジョン:

これは、このファームウェアでの最初のバージョンです。

以前のリビジョン:

これは、このファームウェアでの最初のバージョンです。

ファームウェアの依存関係:

なし

改善点/新しい機能:

これは、このファームウェアでの最初のバージョンです。

修正された問題点:

なし

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

拡張

重要な注意:

なし

ファームウェアの依存関係:

なし

改善点/新しい機能:

これは、このファームウェアでの最初のバージョンです。

既知の問題点:

なし

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant DL360 Gen10 (U32)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: cp036781.compsig; cp036781.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant DL360 Gen10システムROM - U32

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバー

に固有のものではありません。

NVDIMM-Nメモリで構成されたシステムで、致命的なプロセッサーエラー状態(IERR)の原因となるシステムクラッシュイベントの発生中に永続データが失われる可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant DL385 Gen10 (A40) サーバー

バージョン: 1.30_06-07-2018 **(推奨)**
ファイル名: cp035120.compsig; cp035120.exe

重要な注意！

重要な注意:

なし

配布名:

HPE ProLiant DL385 Gen10システムROM - A40

リリースバージョン:

1.30_06-07-2018

最新の推奨またはクリティカルリビジョン:

1.30_06-07-2018

以前のリビジョン:

1.22_04-16-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

最新のVMware vSphereセキュアブート証明書のサポートを追加しました。

BIOS/プラットフォーム構成(RBSU)の新しいメモリコントローラーインターリーブメニューを追加しました。このオプションでは、不均衡なメモリ構成で構成されたシステムのメモリパフォーマンスを向上させることができるメモリコントローラーインターリーブを無効にできます。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

システムユーティリティのための言語翻訳(英語以外のモード)をアップデートしました。

修正された問題点:

1TB以上のメモリが取り付けられたシステムにメモリリソースが正しく割り当てられていないため、カーネルパニックが発生したりIOMMUでエラーが報告されたりすることがある問題に対処しました。

UEFI POST検出モードオプションが高速検出の強制に設定されている場合に内蔵Diagnosticsが正しく起動しないことがある問題に対処しました。

システムユーティリティメニューのインテグレーテッドマネジメントログ (IML) ビューアーが起動時に応答しなくなることがある問題に対処しました。

UEFI POST検出モードオプションが高速検出の強制に設定されている場合にHPEデュアルSDカードUSBモジュールが正しく起動しないことがある問題に対処しました。

Trusted Platform Module (TPM) がTPM 2.0モード用に構成されている場合にTPMのファームウェアアップデートが正しく完了しないことがある問題に対処しました。この問題は、TPM 1.2モードで動作するTPMで構成されているシステムには影響しません。

サードパーティのUSBキーがサーバーのUSBポートのいずれかに取り付けられている場合にシステムでIntelligent Provisioningを起動できないことがある問題に対処しました。この問題は特定のUSBキーで検出されたものであり、他のデバイスでは検出されていません。

UEFI POST検出モードオプションが完全検出の強制に設定されている場合にIntegrated Lights-Out (iLO) 仮想メディアが正しく起動しないことがある問題に対処しました。

レガシーブートモードで構成されている場合に、BIOS/プラットフォーム構成(RBSU)から無効にされた内蔵SDカードと、取り付けられているHPEデュアルSDカードで構成されたシステムがHPEデュアルSDカードUSBモジュールから起動しない問題に対処しました。この問題は、UEFIブートモードで構成されているシステムには影響しません。

レガシーブートモードで構成されている場合に、オプションのHPE CN1200E-Tアダプターで構成されたシステムが正しく起動しない問題に対処しました。この問題は、UEFIブートモードで構成されているシステムには影響しません。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

なし

ファームウェアの依存関係:

なし

修正された問題点:

1TB以上のメモリが取り付けられたシステムにメモリリソースが正しく割り当てられていないため、カーネルパニックが発生したりIOMMUでエラーが報告されたりすることがある問題に対処しました。

UEFI POST検出モードオプションが高速検出の強制に設定されている場合に内蔵Diagnosticsが正しく起動しないことがある問題に対処しました。

システムユーティリティメニューのインテグレーテッドマネジメントログ (IML) ビューアーが起動時に応答しなくなることがある問題に対処しました。

UEFI POST検出モードオプションが高速検出の強制に設定されている場合にHPEデュアルSDカードUSBモジュールが正しく起動しないことがある問題に対処しました。

Trusted Platform Module (TPM) がTPM 2.0モード用に構成されている場合にTPMのファームウェアアップデートが正しく完了しないことがある問題に対処しました。この問題は、TPM 1.2モードで動作するTPMで構成されているシステムには影響しません。

サードパーティのUSBキーがサーバーのUSBポートのいずれかに取り付けられている場合にシステムでIntelligent Provisioningを起動できないことがある問題に対処しました。この問題は特定のUSBキーで検出されたものであり、他のデバイスでは検出されていません。

UEFI POST検出モードオプションが完全検出の強制に設定されている場合にIntegrated Lights-Out (iLO) 仮想メディアが正しく起動しないことがある問題に対処しました。

レガシーブートモードで構成されている場合に、BIOS/プラットフォーム構成(RBSU)から無効にされた内蔵SDカードと、取り付けられているHPEデュアルSDカードで構成されたシステムがHPEデュアルSDカードUSBモジュールから起動しない問題に対処しました。この問題は、UEFIブートモードで構成されているシステムには影響しません。

レガシーブートモードで構成されている場合に、オプションのHPE CN1200E-Tアダプターで構成されたシステムが正しく起動しない問題に対処しました。この問題は、UEFIブートモードで構成されているシステムには影響しません。

既知の問題点:

なし

拡張

最新のVMware vSphereセキュアブート証明書のサポートを追加しました。

BIOS/プラットフォーム構成(RBSU)の新しいメモリコントローラーインターリーブメニューを追加しました。このオプションでは、不均衡なメモリ構成で構成されたシステムのメモリパフォーマンスを向上させることができるメモリコントローラーインターリーブを無効にできます。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

システムユーティリティのための言語翻訳(英語以外のモード)をアップデートしました。

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant EC200a (U26) サーバー/HPE ProLiant Thin Micro TM200 (U26) サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp036462.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant Thin Micro TM200サーバーGen9システムROM - U26

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

拡張

なし

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant ML110 Gen10 (U33)サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: cp036767.compsig; cp036767.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML110 Gen10システムROM - U33

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッ

サーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

拡張

なし

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant ML30 Gen9 (U23)サーバー

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035704.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML30 Gen9 システムROM - U23

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant ML350 Gen10 (U41) サーバー

バージョン: 1.42_06-20-2018 **(クリティカル)**
ファイル名: cp036828.compsig; cp036828.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant ML350 Gen10システムROM - U41

リリースバージョン:

1.42_06-20-2018

最新の推奨またはクリティカルリビジョン:

1.42_06-20-2018

以前のリビジョン:

1.40_06-15-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性がありま

す。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このファームウェアバージョンには、システムで、iLO Integrated Management Log(IML)に記録されている「a 389-Unexpected Shutdown and Restart」が発生することがある問題についての追加の修正(バージョン1.40以降)が含まれています。この問題は、HPEサーバーに固有のものではありません。

システムでシステムリセットイベントの発生時に誤ったBank 4マシンチェックがiLO Integrated Management Log(IML)に記録されることがある問題に対処しました。ほとんどの場合、このエラーは無視してもかまいません。この問題は、HPEサーバーに固有のものではありません。

既知の問題点:

なし

オンラインROMフラッシュコンポーネントfor Windows x64 - HPE ProLiant XL270d (U25) アクセラレータトレイ

バージョン: 2.60_05-21-2018 **(クリティカル)**
ファイル名: cp035818.exe

重要な注意！

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

提供名:

HPE ProLiant XL270dアクセラレータトレイシステムROM - U25

リリースバージョン:

2.60_05-21-2018

最新の推奨またはクリティカルリビジョン:

2.60_05-21-2018

以前のリビジョン:

2.56_01-22-2018

ファームウェアの依存関係:

なし

改善点/新しい機能:

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイク

ロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

事前要件

Windows用"HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) は、 Service Pack for ProLiant (SPP) から入手できます。

修正

重要な注意:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

ファームウェアの依存関係:

なし

修正された問題点:

このシステムROMのリビジョンには、オペレーティングシステムとハイパーバイザーのアップデートの組み合わせによって、L1 Terminal Fault – OS/SMM(CVE-2018-3620)およびL1 Terminal Fault – VMM(CVE-2018-3646)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。 このような脆弱性のために、L1データキャッシュに存在している情報が、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に不正に開示されてしまう可能性があります。 こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのサーバーに影響します。 このサーバーは、SGXをサポートしていないので、L1 Terminal Fault – SGX(CVE-2018-3615)(Foreshadowとも呼ばれます)に対して脆弱ではないことに注意してください。

このシステムROMのリビジョンには、オペレーティングシステムのアップデートの組み合わせによって、Speculative Store Bypass(Variant 4とも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3639です。投機的実行機能を利用するマイクロプロセッサーを搭載し、先のすべてのメモリ書き込みのアドレスが判明する前にメモリ読み取りを投機的に実行するシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者に情報が不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

このシステムROMのリビジョンには、Rogue Register Read(Variant 3aとも呼ばれます)のセキュリティ脆弱性の軽減を提供する、Intelマイクロコードの最新のリビジョンが含まれています。この問題には中レベルのCVEが割り当てられており、IDはCVE-2018-3640です。投機的実行機能を利用するマイクロプロセッサーを搭載し、システムレジスタの投機的読み取りを行うシステムでは、サイドチャネル解析を通じて、ローカルユーザーのアクセス権を持つ攻撃者にシステムパラメーターが不正に開示される可能性があります。こうしたセキュリティ上の脆弱性は、HPEサーバーに固有のものではなく、影響を受けたプロセッサーを利用するすべてのシステムに影響します。

訂正不能なQPI(Quick Path Interlink)エラーが正しく報告されず、Integrated Management Logにも記録されない問題に対処しました。以前は、障害が検出されずにシステムが起動中に応答しなくなりました。

インテルXeon E5-2600 v4プロセッサーおよび64GB LRDIMMで構成されたシステムで、高い負荷がかかるとMachine Check ExceptionまたはNMIイベントが発生する可能性がある問題に対処しました。この問題は、HPEサーバーに固有のものではありません。

ソフトウェアイニシエーターiSCSIのHPE RESTful設定がリソースレジストリ内で使用できない可能性がある問題に対処しました。

既知の問題点:

なし

拡張

プロセッサーの電力と使用状況のサポートが無効になっているときに、ROMベースセットアップユーティリティ(RBSU)のパワーレギュレーター設定をスタティックローモードまたはOS制御モードに設定できるようにするサポートを追加しました。以前のROMでは、パワーレギュレーターをスタティックハイモード用にのみ構成する必要がありました。

最新のBIOS/プラットフォーム構成オプションと一致するようにRESTful API HPE BIOS属性レジストリリソースをアップデートしました。

ドライバー - チップセット

先頭

Intel Xeon Processor Scalable Family for Windows Server 2012 R2およびServer 2016用識別子

バージョン: 10.1.2.86 (B) **(オプション)**
ファイル名: cp034634.compsig; cp034634.exe

修正

Windows Device Guardが有効になっているときに発生する可能性のあるインストール エラーを修正しました。

Windows用AMD EPYCプロセッサーの識別子
バージョン: 1.0.0.0 (C) **(オプション)**
ファイル名: cp034065.compsig; cp034065.exe

拡張

- HPE ProLiant DL325 Gen10のサポートを追加しました。
- バージョンコントロールDLLの著作権の文字列を修正しました。

ドライバー - ネットワーク 先頭

Windows Server 2012 R2用HPE Intel ixsドライバー
バージョン: 3.14.75.0 **(オプション)**
ファイル名: cp033709.compsig; cp033709.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.2.2以降で提供されるファームウェアを推奨しています。

拡張

このドライバーは、最新のNDISドライバーとの互換性を維持するために更新されています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

Windows Server 2012 R2用HPE Intel v40eドライバー
バージョン: 1.5.76.0 **(オプション)**
ファイル名: cp034522.compsig; cp034522.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

事前要件

このドライバーではホストドライバーバージョン1.8.90.0以降が必要です。

サポートしているデバイスおよび機能

この製品は、以下のHPE Intel i40eaネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター

HP Emulex 10/20GbE iSCSIドライバー for Red Hat Enterprise Linux 6 x86_64
バージョン: 12.0.1110.21-1 **(オプション)**

ファイル名: kmod-be2iscsi-12.0.1110.21-1.rhel6u8.x86_64.compsig; kmod-be2iscsi-12.0.1110.21-1.rhel6u8.x86_64.rpm; kmod-be2iscsi-12.0.1110.21-1.rhel6u9.x86_64.compsig; kmod-be2iscsi-12.0.1110.21-1.rhel6u9.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Linux(x64)*、バージョン2018.09.01で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HP Emulex 10/20GbEドライバー for Red Hat Enterprise Linux 6 x86_64

バージョン: 12.0.1110.20-1 **(オプション)**
ファイル名: kmod-be2net-12.0.1110.20-1.rhel6u8.x86_64.compsig; kmod-be2net-12.0.1110.20-1.rhel6u8.x86_64.rpm; kmod-be2net-12.0.1110.20-1.rhel6u9.x86_64.compsig; kmod-be2net-12.0.1110.20-1.rhel6u9.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Linux(x64)*、バージョン2018.09.01で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HP Mellanox RoCE (RDMA over Converged Ethernet)ドライバー for Red Hat Enterprise Linux 6 Update 8 (x86_64)

バージョン: 4.3 **(推奨)**
ファイル名: 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

重要な注意！

Mellanox Ethernet + RoCE Linuxドライバー(mlnx-ofa_kernel RPM)は、HPE MellanoxアダプターのEthernet動作モードのみサポートします。完全なInfiniBand機能または"InfiniBand + Ethernet"動作モードを同じノード上で必要とする場合、"Mellanox OFED VPI Drivers and Utilities"というLinuxソフトウェア配信リポジトリ(https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/)からMLNX-OFEDドライバーをインストールしてください。

修正

バージョン4.1で、以下の問題を解決しました。

- IPv6のプロシージャーが、基となるカーネルでサポートされていないときに呼び出されました。
- カーネル4.11で始まったメモリーリークの問題を修正し、将来のSKBリークの検出を容易にするために、Soft RoCEドライバーに警告メッセージを追加しました。
- RXeデバイスを仮想(ダミー)デバイスと組み合わせたときに、カーネルのクラッシュがしばしば発生していました。
- IPベースのGIDの損失が原因で、RoCE GIDキャッシュの競合状態がしばしば生じていました。
- 同じホスト上のクライアントとサーバー間のrdma_cm接続は、VLANインターフェイスを介して操作しているときは不可能でした。
- RDMACM接続の接続レートが高いときは、RDMA_CM_EVENT_UNREACHABLEというエラーメッセージが 表示されて失敗することがよくありました。
- ページサイズが16KBより大きいシステムでは、SR-IOV(シングルルートI/O仮想化)はサポートされていませんでした。

バージョン4.0で、以下の問題を解決しました。

- SLES12 SP2でドライバーの起動時にカーネルがメモリ不足になることがありました。
- MACアドレス00:00:00:00:00:00でスプーフィングチェックがオンになりました
- Large Receive Offload (LRO)がオンになっていたときにTCPパケットが不適切な方法で受信されました。
- RXリングサイズを大きくするとCQバッファーのメモリ割り当てが失敗することがよくありました。
- MLNX_ENドライバーが4KページのARMアーキテクチャーでロードに失敗しました。

バージョン3.4で、以下の問題を解決しました。

- mlx4_ibモジュールがロードされなかった場合、タイムアウト後の "ethtool" セルフテストが割り込みテストで失敗することがありました。
- まれな状況で、非同期のイベントハンドラーから呼ばれたmlx4_en_get_drvinfo() によって、システムリブートの間にカーネルパニックが発生することがありました。
- VF netdevsが開いている状態でSR-IOVを無効にしようとすると、操作が失敗しました。

拡張

HPE Mellanox RoCEドライバーv4.1は、以下の変更点および新機能を含みます。

- /sys/class/infiniband/mlx5_0/ports/1/hw_counters/ディレクトリの下にある追加のRoCE診断およびECN輻輳カウンターのサポート。
- rx-fcs ethtoolオフロード構成のサポート。通常、パケットのFCSは、アプリケーションソケットバッファー(skb)に送信される前にASICハードウェアによって切り捨てられます。Ethtoolを使用して、rx-fcsが切り捨てられないように設定しながら、分析のためにアプリケーションに渡すことができます。
- DSCP値に基づいてPFCを有効にするためのオプション。この解決方法を使用することで、VLANヘッダーの使用が必須ではなくなります。
- ECNパラメーターは次のディレクトリに移動されています。/sys/kernel/debug/mlx5//cc_params/
- mlx_fs_dump(ステアリングルールを読み出し可能な形式で出力するpythonツール)のサポート。
- 名前やIDなどのPCIピア属性を指定する際に、デバイスをオープンし、コンテキストを作成する機能。
- ハイパーバイザー上の検査済みVFを無効する機能。
- ローカルループバックが使用されていないときに、ローカルループバック(ユニキャストおよびマルチキャスト)をmlx5ドライバーによってデフォルトで無効にすることで、パフォーマンスを改善しました。mlx5ドライバーは、ユーザースペースのアプリケーションによって開いた伝送ドメインの数を記録します。複数のユーザースペースの伝送ドメインが開いている場合、ローカルループバックは自動的に有効になります。
- 1パルス/秒(1PPS)のサポート。これは、アダプターがアダプターカードの専用のピンで1パルス/秒を送受信できるようにする時刻同期機能です。
- シャットダウンおよびkexecフローでのドライバーの高速終了のサポート。
- NVMe over Fabrics (NVMEoF)オフロード(ハードウェアの新しいNVMEoF標準ターゲット(サーバー)側の実装)のサポート。
- デフォルトのRoCEモードを変更して、RDMA CMがRoCEv1ではなくRoCEv2で利用できるようにしました。クライアント側とサーバー側で同じRoCEモードをサポートするには、RDMA_CMセッションに両方の側が必要です。そうでない場合、クライアントはサーバーに接続できなくなります。

HPE Mellanox RoCEドライバーバージョン3.4は、以下の変更点および新機能を含みます。

- 以下のカーネルモジュールパラメーターを追加しました:
  - mlx4_en_only_mode
  - udev_dev_port_dev_id

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるRed Hat Enterprise Linux 6U8 (x86_64)のカーネルは、次のとおりです。
2.6.32-642.el6 - (x86_64) および将来アップデートされるカーネル。

HP Mellanox RoCE (RDMA over Converged Ethernet)ドライバー for Red Hat Enterprise Linux 6 Update 9 (x86_64)

バージョン: 4.3 **(推奨)**
ファイル名: 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

重要な注意！

Mellanox Ethernet + RoCE Linuxドライバー(mlnx-ofa_kernel RPM)は、HPE MellanoxアダプターのEthernet動作モードのみサポートします。完全なInfiniBand機能または"InfiniBand + Ethernet"動作モードを同じノード上で必要とする場合、"Mellanox OFED VPI Drivers and Utilities"というLinuxソフトウェア配信リポジトリ(https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/)からMLNX-OFEDドライバーをインストールしてください。

修正

バージョン4.1で、以下の問題を解決しました。

- IPv6のプロシージャーが、基となるカーネルでサポートされていないときに呼び出されました。
- カーネル4.11で始まったメモリーリークの問題を修正し、将来のSKBリークの検出を容易にするために、Soft RoCEドライバーに警告メッセージを追加しました。
- RXeデバイスを仮想(ダミー)デバイスと組み合わせたときに、カーネルのクラッシュがしばしば発生していました。
- IPベースのGIDの損失が原因で、RoCE GIDキャッシュの競合状態がしばしば生じていました。
- 同じホスト上のクライアントとサーバー間のrdma_cm接続は、VLANインターフェイスを介して操作しているときは不可能でした。
- RDMACM接続の接続レートが高いときは、RDMA_CM_EVENT_UNREACHABLEというエラーメッセージが 表示されて失敗することがよくありました。
- ページサイズが16KBより大きいシステムでは、SR-IOV(シングルルートI/O仮想化)はサポートされていませんでした。

バージョン4.0で、以下の問題を解決しました。

- SLES12 SP2でドライバーの起動時にカーネルがメモリ不足になることがありました。
- MACアドレス00:00:00:00:00:00でスプーフィングチェックがオンになりました
- Large Receive Offload (LRO)がオンになっていたときにTCPパケットが不適切な方法で受信されました。
- RXリングサイズを大きくするとCQバッファーのメモリ割り当てが失敗することがよくありました。
- MLNX_ENドライバーが4KページのARMアーキテクチャーでロードに失敗しました。

バージョン3.4で、以下の問題を解決しました。

- mlx4_ibモジュールがロードされなかった場合、タイムアウト後の "ethtool" セルフテストが割り込みテストで失敗することがありました。
- まれな状況で、非同期のイベントハンドラーから呼ばれたmlx4_en_get_drvinfo() によって、システムリブートの間にカーネルパニックが発生することがありました。
- VF netdevsが開いている状態でSR-IOVを無効にしようとすると、操作が失敗しました。

拡張

HPE Mellanox RoCEドライバーv4.1は、以下の変更点および新機能を含みます。

- /sys/class/infiniband/mlx5_0/ports/1/hw_counters/ディレクトリの下にある追加のRoCE診断およびECN輻輳カウンターのサポート。
- rx-fcs ethtoolオフロード構成のサポート。通常、パケットのFCSは、アプリケーションソケットバッファー(skb)に送信される前にASICハードウェアによって切り捨てられます。Ethtoolを使用して、rx-fcsが切り捨てられないように設定しながら、分析のためにアプリケーションに渡すことができます。
- DSCP値に基づいてPFCを有効にするためのオプション。この解決方法を使用することで、VLANヘッダーの使用が必須ではなくなります。
- ECNパラメーターは次のディレクトリに移動されています。/sys/kernel/debug/mlx5//cc_params/
- mlx_fs_dump(ステアリングルールを読み出し可能な形式で出力するpythonツール)のサポート。
- 名前やIDなどのPCIピア属性を指定する際に、デバイスをオープンし、コンテキストを作成する機能。
- ハイパーバイザー上の検査済みVFを無効する機能。
- ローカルループバックが使用されていないときに、ローカルループバック(ユニキャストおよびマルチキャスト)をmlx5ドライバーによってデフォルトで無効にすることで、パフォーマンスを改善しました。mlx5ドライバーは、ユーザースペースのアプリケーションによって開いた伝送ドメインの数を記録します。複数のユーザースペースの伝送ドメインが開いている場合、ローカルループバックは自動的に有効になります。
- 1パルス/秒(1PPS)のサポート。これは、アダプターがアダプターカードの専用のピンで1パルス/秒を送受信できるようにする時刻同期機能です。
- シャットダウンおよびkexecフローでのドライバーの高速終了のサポート。
- NVMe over Fabrics (NVMEoF)オフロード(ハードウェアの新しいNVMEoF標準ターゲット(サーバー)側の実装)のサポート。
- デフォルトのRoCEモードを変更して、RDMA CMがRoCEv1ではなくRoCEv2で利用できるようにしました。クライアント側とサーバー側で同じRoCEモードをサポートするには、RDMA_CMセッションに両方の側が必要です。そうでない場合、クライアントはサーバーに接続できなくなります。

HPE Mellanox RoCEドライバーバージョン3.4は、以下の変更点および新機能を含みます。

- 以下のカーネルモジュールパラメーターを追加しました:
  - mlx4_en_only_mode
  - udev_dev_port_dev_id

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるRed Hat Enterprise Linux 6 Update 9 (x86_64)カーネルは、次の通りです。
2.6.32-696.el6 - (x86_64) および将来アップデートされるカーネル。

HPE Broadcom NetXtreme-E RoCE Library for SUSE Linux Enterprise Server 12 SP2

バージョン: 212.0.82.0 **(オプション)**
ファイル名: libbnxtre-212.0.82.0-sles12sp2.x86_64.compsig; libbnxtre-212.0.82.0-sles12sp2.x86_64.rpm; README

事前要件

この製品をインストールする前に、*HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6*、バージョン1.9.1-212.0.99.0以降をインストールする必要があります。

RoCEライブラリをインストールする前に、ターゲットシステムにlibibverbパッケージをインストールしておく必要があります。まだインストールしていない場合は、オペレーティングシステムのインストールメディアからlibibverbパッケージを取得できます。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-E RoCE Library for SUSE Linux Enterprise Server 12 SP2

バージョン: 212.0.82.0 (B) **(推奨)**

ファイル名: libbnxtre-212.0.82.0-sles12sp2.x86_64.compsig; libbnxtre-212.0.82.0-sles12sp2.x86_64.rpm; README

事前要件

この製品をインストールする前に、*HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6*、バージョン1.9.1-212.0.99.0以降をインストールする必要があります。

RoCEライブラリをインストールする前に、ターゲットシステムにlibibverbパッケージをインストールしておく必要があります。まだインストールしていない場合は、オペレーティングシステムのインストールメディアからlibibverbパッケージを取得できます。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-E RoCE Library for SUSE Linux Enterprise Server 12 SP3

バージョン: 212.0.82.0 **(オプション)**

ファイル名: libbnxt_re-212.0.82.0-sles12sp3.x86_64.compsig; libbnxt_re-212.0.82.0-sles12sp3.x86_64.rpm; README

事前要件

この製品をインストールする前に、*HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6*、バージョン1.9.1-212.0.99.0以降をインストールする必要があります。

RoCEライブラリをインストールする前に、ターゲットシステムにlibibverbパッケージをインストールしておく必要があります。まだインストールしていない場合は、オペレーティングシステムのインストールメディアからlibibverbパッケージを取得できます。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-E RoCE Library for SUSE Linux Enterprise Server 12 SP3

バージョン: 212.0.82.0 (B) **(推奨)**

ファイル名: libbnxt_re-212.0.82.0-sles12sp3.x86_64.compsig; libbnxt_re-212.0.82.0-sles12sp3.x86_64.rpm; README

事前要件

この製品をインストールする前に、*HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6*、バージョン1.9.1-212.0.99.0以降をインストールする必要があります。

RoCEライブラリをインストールする前に、ターゲットシステムにlibibverbパッケージをインストールしておく必要があります。まだインストールしていない場合は、オペレーティングシステムのインストールメディアからlibibverbパッケージを取得

できます。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-E ドライバー for SUSE Linux Enterprise Server 11 x86_64

バージョン: 1.9.1-212.0.99.0 (B) **(推奨)**
ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.3.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-E ドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 1.9.1-212.0.99.0 **(オプション)**
ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.3.10以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-E ドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 1.9.1-212.0.99.0 (B) **(推奨)**
ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.3.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-E ドライバー for Windows Server 2016

バージョン: 212.0.89.0 **(オプション)**
ファイル名: cp034200.compsig; cp034200.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-Eドライバーfor Red Hat Enterprise Linux 6

バージョン: 1.9.1-212.0.99.0 (B) **(推奨)**
ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.3.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-Eドライバーfor Red Hat Enterprise Linux 7

バージョン: 1.9.1-212.0.99.0 (B) **(推奨)**
ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.3.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-Eドライバーfor VMware vSphere 6.0

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035284.compsig; cp035284.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for VMware*、バージョン5.5.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-Eドライバーfor VMware vSphere 6.5

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035285.compsig; cp035285.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for VMware*、バージョン5.5.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-Eドライバーfor Windows Server 2012 R2

バージョン: 212.0.89.0 **(オプション)**
ファイル名: cp034199.compsig; cp034199.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Broadcom NetXtreme-E Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NX1 1Gbドライバーfor Windows Server x64 Edition

バージョン: 212.0.0.0 **(オプション)**
ファイル名: cp034731.compsig; cp034731.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Broadcom NX1 Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

修正

このドライバーは、重度の負荷がかかる環境でシステムが動作している場合に、Windows Stop Error (0x133)という結果になる問題を修正します。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 330iアダプター(22BD)
- HP Ethernet 1Gb 4ポート 331iアダプター(22BE)
- HPE Ethernet 1Gb 4ポート 331FLRアダプター
- HPE Ethernet 1Gb 4ポート 331Tアダプター
- HP Ethernet 1Gb 2ポート 332iアダプター(2133)
- HP Ethernet 1Gb 2ポート 332iアダプター(22E8)
- HPE Ethernet 1Gb 2ポート 332Tアダプター

HPE Broadcom tg3 Ethernetドライバー for Red Hat Enterprise Linux 6 x86_64

バージョン: 3.137w-3 **(オプション)**

ファイル名: kmod-tg3-3.137w-3.rhel6u8.x86_64.compsig; kmod-tg3-3.137w-3.rhel6u8.x86_64.rpm; kmod-tg3-3.137w-3.rhel6u9.x86_64.compsig; kmod-tg3-3.137w-3.rhel6u9.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE NX1 Broadcom Online Firmware Upgrade Utility for Linux x86_64*、バージョン2.21.58以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2-port 330iアダプター(22BD)
- HP Ethernet 1Gb 4-port 331iアダプター(22BE)
- HP Ethernet 1Gb 4-port 331FLRアダプター
- HP Ethernet 1Gb 4-port 331Tアダプター
- HP Ethernet 1Gb 2-port 332iアダプター(2133)
- HP Ethernet 1Gb 2-port 332iアダプター(22E8)
- HP Ethernet 1Gb 2-port 332Tアダプター

HPE Broadcom tg3 Ethernetドライバー for Red Hat Enterprise Linux 7 x86_64

バージョン: 3.137w-3 **(オプション)**
ファイル名: kmod-tg3-3.137w-3.rhel7u4.x86_64.compsig; kmod-tg3-3.137w-3.rhel7u4.x86_64.rpm; kmod-tg3-3.137w-3.rhel7u5.x86_64.compsig; kmod-tg3-3.137w-3.rhel7u5.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE NX1 Broadcom Online Firmware Upgrade Utility for Linux x86_64*、バージョン2.21.58以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 330iアダプター(22BD)
- HP Ethernet 1Gb 4ポート 331iアダプター(22BE)
- HP Ethernet 1Gb 4ポート 331FLRアダプター
- HP Ethernet 1Gb 4ポート 331Tアダプター
- HP Ethernet 1Gb 2ポート 332iアダプター(2133)
- HP Ethernet 1Gb 2ポート 332iアダプター(22E8)
- HP Ethernet 1Gb 2ポート 332Tアダプター

HPE Broadcom tg3 Ethernetドライバー for SUSE Linux Enterprise Server 11 x86_64

バージョン: 3.137w-3 **(オプション)**
ファイル名: README; tg3-kmp-default-3.137w_3.0.101_63-3.sles11sp4.x86_64.compsig; tg3-kmp-default-3.137w_3.0.101_63-3.sles11sp4.x86_64.rpm; tg3-kmp-default-3.137w_3.0.76_0.11-3.sles11sp3.x86_64.compsig; tg3-kmp-default-3.137w_3.0.76_0.11-3.sles11sp3.x86_64.rpm; tg3-kmp-xen-3.137w_3.0.101_63-3.sles11sp4.x86_64.compsig; tg3-kmp-xen-3.137w_3.0.101_63-3.sles11sp4.x86_64.rpm; tg3-kmp-xen-3.137w_3.0.76_0.11-3.sles11sp3.x86_64.compsig; tg3-kmp-xen-3.137w_3.0.76_0.11-3.sles11sp3.x86_64.rpm

重要な注意！

これらのドライバーとともに使用する場合は、*HPE NX1 Broadcom Online Firmware Upgrade Utility for Linux x86_64*、バージョン2.21.58以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2-port 330iアダプター(22BD)
- HP Ethernet 1Gb 4-port 331iアダプター(22BE)
- HP Ethernet 1Gb 4-port 331FLRアダプター
- HP Ethernet 1Gb 4-port 331Tアダプター
- HP Ethernet 1Gb 2-port 332iアダプター(2133)
- HP Ethernet 1Gb 2-port 332iアダプター(22E8)
- HP Ethernet 1Gb 2-port 332Tアダプター

HPE Broadcom tg3 Ethernetドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 3.137w-1 **(オプション)**
ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE NX1 Broadcom Online Firmware Upgrade Utility for Linux x86_64*、バージョン2.21.3以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 330iアダプター(22BD)
- HP Ethernet 1Gb 4ポート 331iアダプター(22BE)
- HP Ethernet 1Gb 4ポート 331FLRアダプター
- HP Ethernet 1Gb 4ポート 331Tアダプター
- HP Ethernet 1Gb 2ポート 332iアダプター(2133)
- HP Ethernet 1Gb 2ポート 332iアダプター(22E8)
- HP Ethernet 1Gb 2ポート 332Tアダプター

HPE Broadcom tg3 Ethernetドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 3.137w-3 **(オプション)**
ファイル名: README; tg3-kmp-default-3.137w_k4.4.21_69-3.sles12sp2.x86_64.compsig; tg3-kmp-default-3.137w_k4.4.21_69-3.sles12sp2.x86_64.rpm; tg3-kmp-default-3.137w_k4.4.73_5-3.sles12sp3.x86_64.compsig; tg3-kmp-default-3.137w_k4.4.73_5-3.sles12sp3.x86_64.rpm

重要な注意！

これらのドライバーとともに使用する場合は、*HPE NX1 Broadcom Online Firmware Upgrade Utility for Linux x86_64*、バージョン2.21.58以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 330iアダプター(22BD)
- HP Ethernet 1Gb 4ポート 331iアダプター(22BE)
- HP Ethernet 1Gb 4ポート 331FLRアダプター
- HP Ethernet 1Gb 4ポート 331Tアダプター
- HP Ethernet 1Gb 2ポート 332iアダプター(2133)
- HP Ethernet 1Gb 2ポート 332iアダプター(22E8)
- HP Ethernet 1Gb 2ポート 332Tアダプター

HPE Broadcom tg3 Ethernetドライバー for VMware vSphere 6.0

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035307.compsig; cp035307.zip
ドライバー名およびバージョン:

重要な注意！

このドライバーとともに使用する場合は、*HPE Broadcom NX1 Online Firmware Upgrade Utility for VMware*、バージョン1.22.1で提供されるファームウェアを推奨しています。

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hp.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート330iアダプター
- HP Ethernet 1Gb 4-port 331FLRアダプター
- HP Ethernet 1Gb 4ポート 331i アダプター
- HP Ethernet 1Gb 4ポート 331Tアダプター
- HP Ethernet 1Gb 2ポート 332iアダプター(2133)
- HP Ethernet 1Gb 2ポート 332iアダプター(22E8)
- HP Ethernet 1Gb 2ポート 332Tアダプター

HPE Emulex 10/20 GbE iSCSIドライバー for Windows Server 2012

バージョン: 12.0.1104.0 **(オプション)**
ファイル名: cp034401.compsig; cp034401.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Windows(x64)*、バージョン2018.06.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20 GbE iSCSIドライバー for Windows Server 2012 R2

バージョン: 12.0.1104.0 **(オプション)**
ファイル名: cp034402.compsig; cp034402.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Windows(x64)*、バージョン2018.06.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20 GbE iSCSIドライバー for Windows Server 2016

バージョン: 12.0.1104.0 **(オプション)**
ファイル名: cp034403.compsig; cp034403.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Windows(x64)*、バージョン2018.06.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20 GbE iSCSIドライバーfor VMware vSphere 6.0

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035283.compsig; cp035283.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters for VMware vSphere 6.0*、バージョン2018.09.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20 GbEドライバー for VMware vSphere 6.5

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035290.compsig; cp035290.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters for VMware vSphere 6.5*、バージョン2018.09.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20 GbEドライバー for Windows Server 2012

バージョン: 12.0.1115.0 **(オプション)**
ファイル名: cp034398.compsig; cp034398.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Windows(x64)*、バージョン2018.06.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20 GbEドライバー for Windows Server 2012 R2

バージョン: 12.0.1115.0 **(オプション)**
ファイル名: cp034399.compsig; cp034399.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Windows(x64)*、バージョン2018.06.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20 GbEドライバーfor Windows Server 2016

バージョン: 12.0.1115.0 **(オプション)**
ファイル名: cp034400.compsig; cp034400.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Windows(x64)*、バージョン2018.06.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20GbE iSCSI ドライバー for SUSE Linux Enterprise Server 11 x86_64

バージョン: 12.0.1110.21-1 **(オプション)**
ファイル名: be2iscsi-kmp-default-12.0.1110.21_3.0.101_63-1.sles11sp4.x86_64.compsig; be2iscsi-kmp-default-12.0.1110.21_3.0.101_63-1.sles11sp4.x86_64.rpm; be2iscsi-kmp-default-12.0.1110.21_3.0.76_0.11-1.sles11sp3.x86_64.compsig; be2iscsi-kmp-default-12.0.1110.21_3.0.76_0.11-1.sles11sp3.x86_64.rpm; be2iscsi-kmp-xen-12.0.1110.21_3.0.101_63-1.sles11sp4.x86_64.compsig; be2iscsi-kmp-xen-12.0.1110.21_3.0.101_63-1.sles11sp4.x86_64.rpm; be2iscsi-kmp-xen-12.0.1110.21_3.0.76_0.11-1.sles11sp3.x86_64.compsig; be2iscsi-kmp-xen-12.0.1110.21_3.0.76_0.11-1.sles11sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Linux(x64)*、バージョン2018.09.01で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20GbE iSCSI ドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 12.0.1110.11-1 **(オプション)**

ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Linux(x64)*、バージョン2018.06.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20GbE iSCSI ドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 12.0.1110.21-1 **(オプション)**

ファイル名: be2iscsi-kmp-default-12.0.1110.21_k4.4.103_6.38-1.sles12sp3MU5.x86_64.compsig; be2iscsi-kmp-default-12.0.1110.21_k4.4.103_6.38-1.sles12sp3MU5.x86_64.rpm; be2iscsi-kmp-default-12.0.1110.21_k4.4.21_69-1.sles12sp2.x86_64.compsig; be2iscsi-kmp-default-12.0.1110.21_k4.4.21_69-1.sles12sp2.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Linux(x64)*、バージョン2018.09.01で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20GbE iSCSIドライバー for Red Hat Enterprise Linux 7 x86_64

バージョン: 12.0.1110.21-1 **(オプション)**

ファイル名: kmod-be2iscsi-12.0.1110.21-1.rhel7u4.x86_64.compsig; kmod-be2iscsi-12.0.1110.21-1.rhel7u4.x86_64.rpm; kmod-be2iscsi-12.0.1110.21-1.rhel7u5.x86_64.compsig; kmod-be2iscsi-12.0.1110.21-1.rhel7u5.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Linux(x64)*、バージョン2018.09.01で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20GbE iSCSIドライバーfor VMware vSphere 6.5

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035287.compsig; cp035287.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters for VMware vSphere 6.5*、バージョン2018.09.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20GbE ドライバー for Red Hat Enterprise Linux 7 x86_64

バージョン: 12.0.1110.20-1 **(オプション)**
ファイル名: kmod-be2net-12.0.1110.20-1.rhel7u4.x86_64.compsig; kmod-be2net-12.0.1110.20-1.rhel7u4.x86_64.rpm; kmod-be2net-12.0.1110.20-1.rhel7u5.x86_64.compsig; kmod-be2net-12.0.1110.20-1.rhel7u5.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Linux(x64)*、バージョン2018.09.01で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20GbE ドライバー for SUSE Linux Enterprise Server 11 x86_64

バージョン: 12.0.1110.20-1 **(オプション)**

ファイル名: be2net-kmp-default-12.0.1110.20_3.0.101_63-1.sles11sp4.x86_64.compsig; be2net-kmp-default-12.0.1110.20_3.0.101_63-1.sles11sp4.x86_64.rpm; be2net-kmp-default-12.0.1110.20_3.0.76_0.11-1.sles11sp3.x86_64.compsig; be2net-kmp-default-12.0.1110.20_3.0.76_0.11-1.sles11sp3.x86_64.rpm; be2net-kmp-xen-12.0.1110.20_3.0.101_63-1.sles11sp4.x86_64.compsig; be2net-kmp-xen-12.0.1110.20_3.0.101_63-1.sles11sp4.x86_64.rpm; be2net-kmp-xen-12.0.1110.20_3.0.76_0.11-1.sles11sp3.x86_64.compsig; be2net-kmp-xen-12.0.1110.20_3.0.76_0.11-1.sles11sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Linux(x64)*、バージョン2018.09.01で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20GbEドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 12.0.1110.11-1 **(オプション)**

ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Linux(x64)*、バージョン2018.06.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10/20GbEドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 12.0.1110.20-1 **(オプション)**

ファイル名: be2net-kmp-default-12.0.1110.20_k4.4.103_6.38-1.sles12sp3MU5.x86_64.compsig; be2net-kmp-default-12.0.1110.20_k4.4.103_6.38-1.sles12sp3MU5.x86_64.rpm; be2net-kmp-default-12.0.1110.20_k4.4.21_69-1.sles12sp2.x86_64.compsig; be2net-kmp-default-12.0.1110.20_k4.4.21_69-1.sles12sp2.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters - Linux(x64)*、バージョン2018.09.01で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Emulex 10GbEドライバーfor VMware vSphere 6.0

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035289.compsig; cp035289.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Firmware Flash for Emulex Converged Network Adapters for VMware vSphere 6.0*、バージョン2018.09.01以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター

HPE Intel E1Rドライバー for Windows Server 2012

バージョン: 12.14.8.0 **(オプション)**
ファイル名: cp028837.exe

重要な注意！

HPEは、これらのドライバー用に *HPE Intel*オンラインファームウェアアップグレードユーティリティ*for Windows Server x64 Editions*、バージョン5.0.0.25またはそれ以降で提供されるファームウェアを推奨します。

修正

このドライバーは、アダプター名が含まれているPowerShellコマンドの失敗につながる問題に対処しています。

サポートしているデバイスおよび機能

このドライバーは、以下のHPE Intel E1Rネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート361iアダプター
- HP Ethernet 1Gb 2ポート 361FLBアダプター
- HP Ethernet 1Gb 2ポート361Tアダプター
- HP Ethernet 1Gb 2ポート363iアダプター
- HP Ethernet 1Gb 1ポート 364i アダプター
- HP Ethernet 1Gb 4ポート 366i アダプター
- HP Ethernet 1Gb 4ポート366FLRアダプター
- HP Ethernet 1Gb 4ポート 366M アダプター
- HP Ethernet 1Gb 4ポート366Tアダプター
- HP Ethernet 1Gb 2ポート367iアダプター

HPE Intel E1Rドライバー for Windows Server 2012 R2

バージョン: 12.14.8.0 **(オプション)**
ファイル名: cp028838.exe

重要な注意！

HPEは、これらのドライバー用に *HPE Intel*オンラインファームウェアアップグレードユーティリティ*for Windows Server x64 Editions*、バージョン5.0.0.25またはそれ以降で提供されるファームウェアを推奨します。

修正

このドライバーは、アダプター名が含まれているPowerShellコマンドの失敗につながる問題に対処しています。

拡張

この製品は、HPE Ethernet 1Gb 4ポート 366i コミュニケーションボードをサポートします。

サポートしているデバイスおよび機能

このドライバーは、以下のHPE Intel E1Rネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート361iアダプター
- HP Ethernet 1Gb 2ポート 361FLBアダプター
- HP Ethernet 1Gb 2ポート361Tアダプター
- HP Ethernet 1Gb 2ポート363iアダプター
- HP Ethernet 1Gb 1ポート 364i アダプター
- HP Ethernet 1Gb 4ポート 366i アダプター
- HPE Ethernet 1 Gb 4ポート366i通信ボード
- HP Ethernet 1Gb 4ポート366FLRアダプター
- HP Ethernet 1Gb 4ポート 366M アダプター
- HP Ethernet 1Gb 4ポート366Tアダプター
- HP Ethernet 1Gb 2ポート367iアダプター

HPE Intel E1Rドライバー for Windows Server 2016

バージョン: 12.15.184.0 (B) **(オプション)**
ファイル名: cp031179.compsig; cp031179.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.0.4以降で提供されるファームウェアを推奨しています。

拡張

TBD

サポートしているデバイスおよび機能

このドライバーは、以下のHPE Intel E1Rネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2-port 361iアダプター
- HPE Ethernet 1Gb 2-port 361Tアダプター
- HP Ethernet 1Gb 2-port 363iアダプター
- HP Ethernet 1Gb 1-port 364i アダプター
- HP Ethernet 1Gb 4-port 366i アダプター
- HPE Ethernet 1Gb 4-port 366i通信ボード
- HPE Ethernet 1Gb 4-port 366FLRアダプター
- HPE Ethernet 1Gb 4-port 366Mアダプター
- HPE Ethernet 1Gb 4-port 366Tアダプター

HPE Intel i40eaドライバー for Windows Server 2012

バージョン: 1.8.94.0 **(オプション)**
ファイル名: cp034516.compsig; cp034516.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2-port 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2-port 562SFP+アダプター

HPE Intel i40eaドライバー for Windows Server 2012 R2

バージョン: 1.8.94.0 **(オプション)**
ファイル名: cp034517.compsig; cp034517.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2-port 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2-port 562SFP+アダプター

HPE Intel i40eaドライバー for Windows Server 2016

バージョン: 1.8.94.0 **(オプション)**
ファイル名: cp034518.compsig; cp034518.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2-port 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2-port 562SFP+アダプター

HPE Intel i40ebドライバー for Windows Server 2012 R2

バージョン: 1.8.94.0 **(オプション)**
ファイル名: cp034519.compsig; cp034519.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

修正

このドライバーは、重度の負荷がかかる環境でシステムが動作している場合に、Stop Error (0x133)という結果になる問題を修正します。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

HPE Intel i40ebドライバー for Windows Server 2016

バージョン: 1.8.94.0 **(オプション)**
ファイル名: cp034520.compsig; cp034520.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

修正

このドライバーは、重度の負荷がかかる環境でシステムが動作している場合に、Stop Error (0x133)という結果になる問題を修正します。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター

- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

HPE Intel i40enドライバーfor VMware vSphere 6.5

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035293.compsig; cp035293.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for VMware*、バージョン3.8.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター

HPE Intel i40evfドライバー for Red Hat Enterprise Linux 6 x86_64

バージョン: 3.5.6.1-8 **(推奨)**
ファイル名: kmod-hp-i40evf-3.5.6.1-8.rhel6u8.x86_64.compsig; kmod-hp-i40evf-3.5.6.1-8.rhel6u8.x86_64.rpm; kmod-hp-i40evf-3.5.6.1-8.rhel6u9.x86_64.compsig; kmod-hp-i40evf-3.5.6.1-8.rhel6u9.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 563i アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

HPE Intel i40evfドライバー for Red Hat Enterprise Linux 7 x86_64

バージョン: 3.5.6.1-8 **(推奨)**
ファイル名: kmod-hp-i40evf-3.5.6.1-8.rhel7u4.x86_64.compsig; kmod-hp-i40evf-3.5.6.1-8.rhel7u4.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 563i アダプター
- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

HPE Intel i40evfドライバー for SUSE Linux Enterprise Server 11 x86_64

バージョン: 3.5.6.1-8 **(推奨)**
ファイル名: hp-i40evf-kmp-default-3.5.6.1_k3.0.101_63-8.sles11sp4.x86_64.compsig; hp-i40evf-kmp-default-3.5.6.1_k3.0.101_63-8.sles11sp4.x86_64.rpm; hp-i40evf-kmp-default-3.5.6.1_k3.0.76_0.11-8.sles11sp3.x86_64.compsig; hp-i40evf-kmp-default-3.5.6.1_k3.0.76_0.11-8.sles11sp3.x86_64.rpm; hp-i40evf-kmp-xen-3.5.6.1_k3.0.101_63-8.sles11sp4.x86_64.compsig; hp-i40evf-kmp-xen-3.5.6.1_k3.0.101_63-8.sles11sp4.x86_64.rpm; hp-i40evf-kmp-xen-3.5.6.1_k3.0.76_0.11-8.sles11sp3.x86_64.compsig; hp-i40evf-kmp-xen-3.5.6.1_k3.0.76_0.11-8.sles11sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 563i アダプター
- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

HPE Intel i40evfドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 3.5.6.1-5 **(オプション)**
ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.9以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 563i アダプター
- HPE Ethernet 1Gb 2ポート568iアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

HPE Intel i40evfドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 3.5.6.1-8 **(推奨)**
ファイル名: hp-i40evf-kmp-default-3.5.6.1_k4.4.21_69-8.sles12sp2.x86_64.compsig; hp-i40evf-kmp-default-3.5.6.1_k4.4.21_69-8.sles12sp2.x86_64.rpm; hp-i40evf-kmp-default-3.5.6.1_k4.4.73_5-8.sles12sp3.x86_64.compsig; hp-i40evf-kmp-default-3.5.6.1_k4.4.73_5-8.sles12sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 563i アダプター
- HPE Ethernet 1Gb 2ポート568iアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

HPE Intel i40eドライバー for Red Hat Enterprise Linux 7 x86_64

バージョン: 2.4.6.1-7 **(推奨)**
ファイル名: kmod-hp-i40e-2.4.6.1-7.rhel7u4.x86_64.compsig; kmod-hp-i40e-2.4.6.1-7.rhel7u4.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 563i アダプター
- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

HPE Intel i40eドライバー for SUSE Linux Enterprise Server 11 x86_64

バージョン: 2.4.6.1-7 **(推奨)**

ファイル名: hp-i40e-kmp-default-2.4.6.1_k3.0.101_63-7.sles11sp4.x86_64.compsig; hp-i40e-kmp-default-2.4.6.1_k3.0.101_63-7.sles11sp4.x86_64.rpm; hp-i40e-kmp-default-2.4.6.1_k3.0.76_0.11-7.sles11sp3.x86_64.compsig; hp-i40e-kmp-default-2.4.6.1_k3.0.76_0.11-7.sles11sp3.x86_64.rpm; hp-i40e-kmp-xen-2.4.6.1_k3.0.101_63-7.sles11sp4.x86_64.compsig; hp-i40e-kmp-xen-2.4.6.1_k3.0.101_63-7.sles11sp4.x86_64.rpm; hp-i40e-kmp-xen-2.4.6.1_k3.0.76_0.11-7.sles11sp3.x86_64.compsig; hp-i40e-kmp-xen-2.4.6.1_k3.0.76_0.11-7.sles11sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 563i アダプター
- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

HPE Intel i40eドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 2.4.6.1-4 **(オプション)**

ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.9以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター

- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 563i アダプター
- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

HPE Intel i40eドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 2.4.6.1-7 **(推奨)**
ファイル名: hp-i40e-kmp-default-2.4.6.1_k4.4.21_69-7.sles12sp2.x86_64.compsig; hp-i40e-kmp-default-2.4.6.1_k4.4.21_69-7.sles12sp2.x86_64.rpm; hp-i40e-kmp-default-2.4.6.1_k4.4.73_5-7.sles12sp3.x86_64.compsig; hp-i40e-kmp-default-2.4.6.1_k4.4.73_5-7.sles12sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 563i アダプター
- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

HPE Intel i40eドライバーfor VMware vSphere 6.0

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035292.compsig; cp035292.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for VMware*、バージョン3.8.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター

HPE Intel igbnドライバーfor VMware vSphere 6.5

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035305.compsig; cp035305.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for VMware*、バージョン3.8.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 361iアダプター
- HP Ethernet 1Gb 2ポート 361Tアダプター
- HP Ethernet 1Gb 2ポート 363iアダプター
- HP Ethernet 1Gb 1-port 364i アダプター
- HP Ethernet 1Gb 4ポート 366FLRアダプター
- HP Ethernet 1Gb 4ポート 366iアダプター
- HPE Ethernet 1Gb 4ポート 366i通信ボード
- HP Ethernet 1Gb 4ポート 366Mアダプター
- HP Ethernet 1Gb 4ポート 366Tアダプター

HPE Intel igbドライバー for Red Hat Enterprise Linux 6 x86_64

バージョン: 5.3.5.15-7 **(推奨)**
ファイル名: kmod-hp-igb-5.3.5.15-7.rhel6u8.x86_64.compsig; kmod-hp-igb-5.3.5.15-7.rhel6u8.x86_64.rpm; kmod-hp-igb-5.3.5.15-7.rhel6u9.x86_64.compsig; kmod-hp-igb-5.3.5.15-7.rhel6u9.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のIntelネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 361iアダプター
- HP Ethernet 1Gb 2ポート 361Tアダプター
- HP Ethernet 1Gb 2ポート 363iアダプター
- HP Ethernet 1Gb 1-port 364i アダプター
- HP Ethernet 1Gb 4ポート 366FLRアダプター
- HPE Ethernet 1Gb 4ポート 366i通信ボード
- HP Ethernet 1Gb 4ポート 366Mアダプター
- HP Ethernet 1Gb 4ポート 366Tアダプター

HPE Intel igbドライバー for Red Hat Enterprise Linux 7 x86_64

バージョン: 5.3.5.15-7 **(推奨)**

ファイル名: kmod-hp-igb-5.3.5.15-7.rhel7u4.x86_64.compsig; kmod-hp-igb-5.3.5.15-7.rhel7u4.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のIntelネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 361iアダプター
- HP Ethernet 1Gb 2ポート 361Tアダプター
- HP Ethernet 1Gb 2ポート 363iアダプター
- HP Ethernet 1Gb 1-port 364i アダプター
- HP Ethernet 1Gb 4ポート 366FLRアダプター
- HPE Ethernet 1Gb 4ポート 366i通信ボード
- HP Ethernet 1Gb 4ポート 366Mアダプター
- HP Ethernet 1Gb 4ポート 366Tアダプター

HPE Intel igbドライバー for SUSE Linux Enterprise Server 11 x86_64

バージョン: 5.3.5.15-7 **(推奨)**
ファイル名: hp-igb-kmp-default-5.3.5.15_k3.0.101_63-7.sles11sp4.x86_64.compsig; hp-igb-kmp-default-5.3.5.15_k3.0.101_63-7.sles11sp4.x86_64.rpm; hp-igb-kmp-default-5.3.5.15_k3.0.76_0.11-7.sles11sp3.x86_64.compsig; hp-igb-kmp-default-5.3.5.15_k3.0.76_0.11-7.sles11sp3.x86_64.rpm; hp-igb-kmp-xen-5.3.5.15_k3.0.101_63-7.sles11sp4.x86_64.compsig; hp-igb-kmp-xen-5.3.5.15_k3.0.101_63-7.sles11sp4.x86_64.rpm; hp-igb-kmp-xen-5.3.5.15_k3.0.76_0.11-7.sles11sp3.x86_64.compsig; hp-igb-kmp-xen-5.3.5.15_k3.0.76_0.11-7.sles11sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のIntelネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 361iアダプター
- HP Ethernet 1Gb 2ポート 361Tアダプター
- HP Ethernet 1Gb 2ポート 363iアダプター
- HP Ethernet 1Gb 1-port 364i アダプター
- HP Ethernet 1Gb 4ポート 366FLRアダプター
- HP Ethernet 1Gb 4ポート 366iアダプター
- HPE Ethernet 1Gb 4ポート 366i通信ボード
- HP Ethernet 1Gb 4ポート 366Mアダプター
- HP Ethernet 1Gb 4ポート 366Tアダプター

HPE Intel igbドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 5.3.5.15-4 **(オプション)**
ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.9以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のIntelネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 361iアダプター
- HP Ethernet 1Gb 2ポート 361Tアダプター
- HP Ethernet 1Gb 2ポート 363iアダプター
- HP Ethernet 1Gb 1-port 364i アダプター
- HP Ethernet 1Gb 4ポート 366FLRアダプター
- HPE Ethernet 1Gb 4ポート 366i通信ボード
- HP Ethernet 1Gb 4ポート 366Mアダプター
- HP Ethernet 1Gb 4ポート 366Tアダプター

HPE Intel igbドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 5.3.5.15-7 **(推奨)**
ファイル名: hp-igb-kmp-default-5.3.5.15_k4.4.21_69-7.sles12sp2.x86_64.compsig; hp-igb-kmp-default-5.3.5.15_k4.4.21_69-7.sles12sp2.x86_64.rpm; hp-igb-kmp-default-5.3.5.15_k4.4.73_5-7.sles12sp3.x86_64.compsig; hp-igb-kmp-default-5.3.5.15_k4.4.73_5-7.sles12sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のIntelネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 361iアダプター
- HP Ethernet 1Gb 2ポート 361Tアダプター
- HP Ethernet 1Gb 2ポート 363iアダプター
- HP Ethernet 1Gb 1-port 364i アダプター
- HP Ethernet 1Gb 4ポート 366FLRアダプター
- HPE Ethernet 1Gb 4ポート 366i通信ボード
- HP Ethernet 1Gb 4ポート 366Mアダプター
- HP Ethernet 1Gb 4ポート 366Tアダプター

HPE Intel igbドライバーfor VMware vSphere 6.0

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035295.compsig; cp035295.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for VMware*、バージョン3.8.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 361iアダプター
- HP Ethernet 1Gb 2-port 361Tアダプター
- HP Ethernet 1Gb 2ポート 363iアダプター
- HP Ethernet 1Gb 1-port 364i アダプター
- HP Ethernet 1Gb 4-port 366FLRアダプター
- HP Ethernet 1Gb 4ポート 366iアダプター
- HPE Ethernet 1Gb 4-port 366i通信ボード
- HP Ethernet 1Gb 4ポート 366Mアダプター
- HP Ethernet 1Gb 4-port 366Tアダプター

HPE Intel ixgbe ドライバーfor VMware vSphere 6.0

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035297.compsig; cp035297.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for VMware*、バージョン3.8.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2-port 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2-port 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixgbenドライバーfor VMware vSphere 6.5

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035306.compsig; cp035306.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。このコンポーネントは、vmware.comおよびHPE vibsdepot.hpe.com Webページから利用可能なドライバーと同様であり、さらにHPE固有のCP0xxxxx.xmlファイルを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for VMware*、バージョン3.8.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixgbevfドライバー for Red Hat Enterprise Linux 6 x86_64

バージョン: 4.3.3.1-8 **(推奨)**
ファイル名: kmod-hp-ixgbevf-4.3.3.1-8.rhel6u8.x86_64.compsig; kmod-hp-ixgbevf-4.3.3.1-8.rhel6u8.x86_64.rpm; kmod-hp-ixgbevf-4.3.3.1-8.rhel6u9.x86_64.compsig; kmod-hp-ixgbevf-4.3.3.1-8.rhel6u9.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixgbevfドライバー for Red Hat Enterprise Linux 7 x86_64

バージョン: 4.3.3.1-8 **(推奨)**
ファイル名: kmod-hp-ixgbevf-4.3.3.1-8.rhel7u4.x86_64.compsig; kmod-hp-ixgbevf-4.3.3.1-8.rhel7u4.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixgbevfドライバー for SUSE Linux Enterprise Server 11 x86_64

バージョン: 4.3.3.1-8 **(推奨)**

ファイル名: hp-ixgbevf-kmp-default-4.3.3.1_k3.0.101_63-8.sles11sp4.x86_64.compsig; hp-ixgbevf-kmp-default-4.3.3.1_k3.0.101_63-8.sles11sp4.x86_64.rpm; hp-ixgbevf-kmp-default-4.3.3.1_k3.0.76_0.11-8.sles11sp3.x86_64.compsig; hp-ixgbevf-kmp-default-4.3.3.1_k3.0.76_0.11-8.sles11sp3.x86_64.rpm; hp-ixgbevf-kmp-xen-4.3.3.1_k3.0.101_63-8.sles11sp4.x86_64.compsig; hp-ixgbevf-kmp-xen-4.3.3.1_k3.0.101_63-8.sles11sp4.x86_64.rpm; hp-ixgbevf-kmp-xen-4.3.3.1_k3.0.76_0.11-8.sles11sp3.x86_64.compsig; hp-ixgbevf-kmp-xen-4.3.3.1_k3.0.76_0.11-8.sles11sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixgbevfドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 4.3.3.1-5 **(オプション)**

ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.9以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixgbevfドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 4.3.3.1-8 **(推奨)**

ファイル名: hp-ixgbevf-kmp-default-4.3.3.1_k4.4.21_69-8.sles12sp2.x86_64.compsig; hp-ixgbevf-kmp-default-4.3.3.1_k4.4.21_69-8.sles12sp2.x86_64.rpm; hp-ixgbevf-kmp-default-4.3.3.1_k4.4.73_5-8.sles12sp3.x86_64.compsig; hp-ixgbevf-kmp-default-4.3.3.1_k4.4.73_5-8.sles12sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixgbeドライバー for Red Hat Enterprise Linux 6 x86_64

バージョン: 5.3.5.1-8 **(推奨)**
ファイル名: kmod-hp-ixgbe-5.3.5.1-8.rhel6u8.x86_64.compsig; kmod-hp-ixgbe-5.3.5.1-8.rhel6u8.x86_64.rpm; kmod-hp-ixgbe-5.3.5.1-8.rhel6u9.x86_64.compsig; kmod-hp-ixgbe-5.3.5.1-8.rhel6u9.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixgbeドライバー for Red Hat Enterprise Linux 7 x86_64

バージョン: 5.3.5.1-8 **(推奨)**
ファイル名: kmod-hp-ixgbe-5.3.5.1-8.rhel7u4.x86_64.compsig; kmod-hp-ixgbe-5.3.5.1-8.rhel7u4.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター

- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixgbeドライバー for SUSE Linux Enterprise Server 11 x86_64

バージョン: 5.3.5.1-8 **(推奨)**
ファイル名: hp-ixgbe-kmp-default-5.3.5.1_k3.0.101_63-8.sles11sp4.x86_64.compsig; hp-ixgbe-kmp-default-5.3.5.1_k3.0.101_63-8.sles11sp4.x86_64.rpm; hp-ixgbe-kmp-default-5.3.5.1_k3.0.76_0.11-8.sles11sp3.x86_64.compsig; hp-ixgbe-kmp-default-5.3.5.1_k3.0.76_0.11-8.sles11sp3.x86_64.rpm; hp-ixgbe-kmp-xen-5.3.5.1_k3.0.101_63-8.sles11sp4.x86_64.compsig; hp-ixgbe-kmp-xen-5.3.5.1_k3.0.101_63-8.sles11sp4.x86_64.rpm; hp-ixgbe-kmp-xen-5.3.5.1_k3.0.76_0.11-8.sles11sp3.x86_64.compsig; hp-ixgbe-kmp-xen-5.3.5.1_k3.0.76_0.11-8.sles11sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixgbeドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 5.3.5.1-5 **(オプション)**
ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.9以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター

- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixgbeドライバー for SUSE Linux Enterprise Server 12 x86_64

バージョン: 5.3.5.1-8 **(推奨)**
ファイル名: hp-ixgbe-kmp-default-5.3.5.1_k4.4.21_69-8.sles12sp2.x86_64.compsig; hp-ixgbe-kmp-default-5.3.5.1_k4.4.21_69-8.sles12sp2.x86_64.rpm; hp-ixgbe-kmp-default-5.3.5.1_k4.4.73_5-8.sles12sp3.x86_64.compsig; hp-ixgbe-kmp-default-5.3.5.1_k4.4.73_5-8.sles12sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

HPE Intel ixnドライバー for Windows Server 2012

バージョン: 3.14.78.0 **(オプション)**
ファイル名: cp033707.compsig; cp033707.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.2.2以降で提供されるファームウェアを推奨しています。

修正

このドライバーは、1Gパススルーモジュールとのリンクフラップにつながる問題を修正します。

サポートしているデバイスおよび機能

このソフトウェアは、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 560FLBアダプター
- HPE Ethernet 10Gb 2ポート 560FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 560SFP+アダプター
- HPE Ethernet 10Gb 2ポート560Mアダプター

HPE Intel ixnドライバー for Windows Server 2012 R2

バージョン: 3.14.78.0 **(オプション)**
ファイル名: cp033708.compsig; cp033708.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.2.2以降で提供されるファームウェアを推奨しています。

修正

このドライバーは、1Gパススルーモジュールとのリンクフラップにつながる問題を修正します。

サポートしているデバイスおよび機能

このソフトウェアは、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 560FLBアダプター
- HPE Ethernet 10Gb 2ポート 560FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 560SFP+アダプター
- HPE Ethernet 10Gb 2ポート560Mアダプター

HPE Intel ixnドライバー for Windows Server 2016

バージョン: 4.1.77.0 **(オプション)**
ファイル名: cp033706.compsig; cp033706.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.2.2以降で提供されるファームウェアを推奨しています。

修正

このドライバーは、1Gパススルーモジュールとのリンクフラップにつながる問題を修正します。

拡張

This driver is updated to maintain compatibility with latest NDIS drivers.

サポートしているデバイスおよび機能

このソフトウェアは、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 560FLBアダプター
- HPE Ethernet 10Gb 2ポート 560FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 560SFP+アダプター
- HPE Ethernet 10Gb 2ポート560Mアダプター

HPE Intel ixtドライバー for Windows Server 2012

バージョン: 3.14.78.0 **(オプション)**
ファイル名: cp033711.compsig; cp033711.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.2.2以降で提供されるファームウェアを推奨しています。

修正

このドライバーは、1Gパススルーモジュールとのリンクフラップにつながる問題を修正します。

サポートしているデバイスおよび機能

このソフトウェアは、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 561Tアダプター

HPE Intel ixtドライバー for Windows Server 2012 R2

バージョン: 3.14.78.0 **(オプション)**
ファイル名: cp033712.compsig; cp033712.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.2.2以降で提供されるファームウェアを推奨しています。

修正

このドライバーは、1Gパススルーモジュールとのリンクフラップにつながる問題を修正します。

サポートしているデバイスおよび機能

このソフトウェアは、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 561Tアダプター

HPE Intel ixtドライバー for Windows Server 2016

バージョン: 4.1.76.0 **(オプション)**
ファイル名: cp033713.compsig; cp033713.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.2.2以降で提供されるファームウェアを推奨しています。

修正

このドライバーは、1Gパススルーモジュールとのリンクフラップにつながる問題を修正します。

サポートしているデバイスおよび機能

このソフトウェアは、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 561Tアダプター

HPE Intel vxnドライバー for Windows Server 2012

バージョン: 1.0.15.4 **(オプション)**
ファイル名: cp032567.compsig; cp032567.exe

拡張

最初のリリース。

HPE Intel vxnドライバー for Windows Server 2012 R2

バージョン: 1.0.16.1 **(オプション)**
ファイル名: cp032568.compsig; cp032568.exe

拡張

最初のリリース。

HPE Intel vxnドライバー for Windows Server 2016

バージョン: 2.0.210.0 (B) **(オプション)**
ファイル名: cp034732.compsig; cp034732.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このソフトウェアは、以下のHPE Intel ネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 560FLBアダプター
- HPE Ethernet 10Gb 2ポート 560FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 560SFP+アダプター
- HPE Ethernet 10Gb 2ポート560Mアダプター

このソフトウェアは、以下のHPE Intel ネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 561Tアダプター

HPE Mellanox CX3ドライバー for Windows Server 2016

バージョン: 5.35.12978.0 **(オプション)**
ファイル名: cp031850.compsig; cp031850.exe

サポートしているデバイスおよび機能

このドライバーは、以下のHP Mellanox CX3ネットワークアダプターをサポートします。

- HP Ethernet 10G 2-port 546FLR-SFP+アダプター
- HP Ethernet 10G 2-port 546SFP+アダプター
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP アダプター
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP アダプター
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M アダプター
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP アダプター
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+M アダプター
- HP InfiniBand QDR/EN 10Gb Dual Port 544FLR-QSFPアダプター
- HP InfiniBand FDR/EN 10/40Gb Dual Port544QSFPアダプター
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544FLR-QSFPアダプター
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544Mアダプター
- HP InfiniBand QDR/EN 10Gb Dual Port 544Mアダプター
- HP Infiniband QDR/Ethernet 10Gb 2P 544i アダプター

HPE Mellanox CX3ドライバーfor Windows Server 2012

バージョン: 5.35.12978.0 **(オプション)**
ファイル名: cp031560.compsig; cp031560.exe

サポートしているデバイスおよび機能

このドライバーは、下記のHPE Mellanox CX3ネットワークアダプターをサポートします。

- HP Ethernet 10G 2-port 546FLR-SFP+アダプター
- HP Ethernet 10G 2-port 546SFP+アダプター
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP アダプター
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP アダプター
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M アダプター
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP アダプター
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+M アダプター
- HP InfiniBand QDR/EN 10Gb Dual Port 544FLR-QSFPアダプター
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544QSFPアダプター
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544FLR-QSFPアダプター
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544Mアダプター
- HP InfiniBand QDR/EN 10Gb Dual Port 544Mアダプター
- HP Infiniband QDR/Ethernet 10Gb 2P 544i アダプター

HPE Mellanox CX3ドライバーfor Windows Server 2012 R2

バージョン: 5.35.12978.0 **(オプション)**
ファイル名: cp031561.compsig; cp031561.exe

サポートしているデバイスおよび機能

このドライバーは、下記のHPE Mellanox CX3ネットワークアダプターをサポートします。

- HP Ethernet 10G 2-port 546FLR-SFP+アダプター
- HP Ethernet 10G 2-port 546SFP+アダプター
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+QSFP アダプター
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+FLR-QSFP アダプター
- HP InfiniBand FDR/Ethernet 10Gb/40Gb 2-port 544+M アダプター
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+FLR-QSFP アダプター
- HP InfiniBand QDR/Ethernet 10Gb 2-port 544+M アダプター
- HP InfiniBand QDR/EN 10Gb Dual Port 544FLR-QSFPアダプター
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544QSFPアダプター
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544FLR-QSFPアダプター
- HP InfiniBand FDR/EN 10/40Gb Dual Port 544Mアダプター
- HP InfiniBand QDR/EN 10Gb Dual Port 544Mアダプター
- HP Infiniband QDR/Ethernet 10Gb 2P 544i アダプター

HPE Mellanox CX4LXドライバー for Windows Server 2012

バージョン: 1.90.19216.0 **(オプション)**
ファイル名: cp034467.compsig; cp034467.exe

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HPE Ethernet 25Gb 2ポート 640FLR-SFP28 アダプター
- HPE Ethernet 25Gb 2ポート 640SFP28 アダプター
- HPE Synergy 6410C 25/50Gb Ethernetアダプター
- HPE Infiniband FDR/Ethernet 40/50Gb 2ポート547FLR-QSFPアダプター
- HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28アダプター
- HPE InfiniBand EDR/Ethernet 100Gb 2ポート 840QSFP28アダプター

- HPE Infiniband EDR/Ethernet 100Gb 2ポート841QSFP28アダプター
- HPE Ethernet 100Gb 1ポート 842QSFP28 アダプター

HPE Mellanox CX4LXドライバー for Windows Server 2012 R2

バージョン: 1.90.19216.0 **(オプション)**
ファイル名: cp034468.compsig; cp034468.exe

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HPE Ethernet 25Gb 2ポート 640FLR-SFP28 アダプター
- HPE Ethernet 25Gb 2ポート 640SFP28 アダプター
- HPE Synergy 6410C 25/50Gb Ethernetアダプター
- HPE Infiniband FDR/Ethernet 40/50Gb 2ポート547FLR-QSFPアダプター
- HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28アダプター
- HPE InfiniBand EDR/Ethernet 100Gb 2ポート 840QSFP28アダプター
- HPE Infiniband EDR/Ethernet 100Gb 2ポート841QSFP28アダプター
- HPE Ethernet 100Gb 1ポート 842QSFP28 アダプター

HPE Mellanox CX4LXドライバー for Windows Server 2016

バージョン: 1.90.19216.0 **(オプション)**
ファイル名: cp034469.compsig; cp034469.exe

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HPE Ethernet 25Gb 2ポート 640FLR-SFP28 アダプター
- HPE Ethernet 25Gb 2ポート 640SFP28 アダプター
- HPE Synergy 6410C 25/50Gb Ethernetアダプター
- HPE Infiniband FDR/Ethernet 40/50Gb 2ポート547FLR-QSFPアダプター
- HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28アダプター
- HPE InfiniBand EDR/Ethernet 100Gb 2ポート 840QSFP28アダプター
- HPE Infiniband EDR/Ethernet 100Gb 2ポート841QSFP28アダプター
- HPE Ethernet 100Gb 1ポート 842QSFP28 アダプター

HPE Mellanox RoCE (RDMA over Converged Ethernet) ドライバーfor SUSE LINUX Enterprise Server 11 SP4 AMD64/EM64T)

バージョン: 4.3 **(推奨)**
ファイル名: 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

重要な注意！

Mellanox Ethernet + RoCE Linuxドライバー(mlnx-ofa_kernel RPM)は、HPE MellanoxアダプターのEthernet動作モードのみサポートします。完全なInfiniBand機能または"InfiniBand + Ethernet"動作モードを同じノード上で必要とする場合、"Mellanox OFED VPI Drivers and Utilities"というLinuxソフトウェア配信リポジトリ(https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/)からMLNX-OFEDドライバーをインストールしてください。

修正

バージョン4.1で、以下の問題を解決しました。

- IPv6のプロシージャーが、基となるカーネルでサポートされていないときに呼び出されました。
- カーネル4.11で始まったメモリーリークの問題を修正し、将来のSKBリークの検出を容易にするために、Soft RoCEドライバーに警告メッセージを追加しました。
- RXeデバイスを仮想(ダミー)デバイスと組み合わせたときに、カーネルのクラッシュがしばしば発生していました。
- IPベースのGIDの損失が原因で、RoCE GIDキャッシュの競合状態がしばしば生じていました。
- 同じホスト上のクライアントとサーバー間のrdma_cm接続は、VLANインターフェイスを介して操作しているときは不可能でした。
- RDMACM接続の接続レートが高いときは、RDMA_CM_EVENT_UNREACHABLEというエラーメッセージが 表示されて失敗することがよくありました。
- ページサイズが16KBより大きいシステムでは、SR-IOV(シングルルートI/O仮想化)はサポートされていませんでした。

バージョン4.0で、以下の問題を解決しました。

- SLES12 SP2でドライバーの起動時にカーネルがメモリ不足になることがありました。
- MACアドレス00:00:00:00:00:00でスプーフィングチェックがオンになりました
- Large Receive Offload (LRO)がオンになっていたときにTCPパケットが不適切な方法で受信されました。
- RXリングサイズを大きくするとCQバッファーのメモリ割り当てが失敗することがよくありました。
- MLNX_ENドライバーが4KページのARMアーキテクチャーでロードに失敗しました。

以下の問題点がバージョン3.4で修正されました。

- もしmlx4_ibモジュールがロードされなかったとき、タイムアウト後の "ethtool" セルフテストが割り込みテストでしばしば失敗していました。
- まれな状況で、非同期のイベントハンドラーから呼ばれたmlx4_en_get_drvinfo() によって、システムリブートの間にカーネルパニックが発生することがありました。
- VF netdevsが開いている状態でSR-IOVを無効にしようとすると、操作が失敗しました。

以下の問題が、バージョン3.3 (A)　で修正されました。

- インターフェイスの名前を変更する際の "mlnx_interface_mgr.sh" スクリプトとudevフロー間の競合状態

以下の問題点がバージョン3.3で修正されました。

- SLES12 SP1でのドライバーロードの問題を修正するために互換性 ocrdma.koモジュールを追加しました。
- /sys/class/infiniband//ports// で発見されたエラーカウンターが、ConnectX-4 アダプターカード内で正しく機能しませんでした。
- TXキューカウンター形式を: xq_[tc]*[ring/channel]に変更しました。
- RDMA Sniffer機能の問題を修正しました。
- 仮想機能がethtoolファシリティで使用されている場合、エラーメッセージがログに出力されました。
- 物理リンクのダウン時、同じポート上での物理機能から、任意の仮想機能へのトラフィックが欠落していました。

バージョン3.2 (A) での修正:

- "infiniband support"グループにOS配布のRPMがすでにインストールされている場合、RoCEユーザースペースのライブラリであるRPM "mlnx-ofa_kernel"でインストールに失敗しました。
- 以前のバージョンのMLNX-ENドライバーがすでにインストールされている場合、RoCEドライバーアップグレードが正しく動作しません。これは、Mellanox Ethernet ポートが動作しない原因となります。

バージョン3.2での修正:

- もっとも近い NUMA ノードを、受信側スケーリング用のデフォルトに設定します。
- GROが有効になったときに、プロキシVXLANインターフェイスが正しく処理されないARP要求パケット。

拡張

HPE Mellanox RoCEドライバーv4.1は、以下の変更点および新機能を含みます。

- /sys/class/infiniband/mlx5_0/ports/1/hw_counters/ディレクトリの下にある追加のRoCE診断およびECN輻輳カウンターのサポート。
- rx-fcs ethtoolオフロード構成のサポート。通常、パケットのFCSは、アプリケーションソケットバッファー(skb)に送信される前にASICハードウェアによって切り捨てられます。Ethtoolを使用して、rx-fcsが切り捨てられないように設定し

ながら、分析のためにアプリケーションに渡すことができます。
- DSCP値に基づいてPFCを有効にするためのオプション。この解決方法を使用することで、VLANヘッダーの使用が必須ではなくなります。
- ECNパラメーターは次のディレクトリに移動されています。/sys/kernel/debug/mlx5//cc_params/
- mlx_fs_dump(ステアリングルールを読み出し可能な形式で出力するpythonツール)のサポート。
- 名前やIDなどのPCIピア属性を指定する際に、デバイスをオープンし、コンテキストを作成する機能。
- ハイパーバイザー上の検査済みVFを無効する機能。
- ローカルループバックが使用されていないときに、ローカルループバック(ユニキャストおよびマルチキャスト)をmlx5ドライバーによってデフォルトで無効にすることで、パフォーマンスを改善しました。mlx5ドライバーは、ユーザースペースのアプリケーションによって開いた伝送ドメインの数を記録します。複数のユーザースペースの伝送ドメインが開いている場合、ローカルループバックは自動的に有効になります。
- 1パルス/秒(1PPS)のサポート。これは、アダプターがアダプターカードの専用のピンで1パルス/秒を送受信できるようにする時刻同期機能です。
- シャットダウンおよびkexecフローでのドライバーの高速終了のサポート。
- NVMe over Fabrics (NVMEoF)オフロード(ハードウェアの新しいNVMEoF標準ターゲット(サーバー)側の実装)のサポート。
- デフォルトのRoCEモードを変更して、RDMA CMがRoCEv1ではなくRoCEv2で利用できるようにしました。クライアント側とサーバー側で同じRoCEモードをサポートするには、RDMA_CMセッションに両方の側が必要です。そうでない場合、クライアントはサーバーに接続できなくなります。

HPE Mellanox RoCEドライバーバージョン3.4は、以下の変更点および新機能を含みます。

- 以下のカーネルモジュールパラメーターを追加しました:
  - mlx4_en_only_mode
  - udev_dev_port_dev_id

HPE Mellanox RoCEドライバーv3.3は、以下の変更点および新機能を含みます。

- 修正のみ。

HPE Mellanox RoCEドライバーv3.2は、以下の変更点および新機能を含みます。

- ローパケットキューペアおよび作業キュー用のFCS分散。
- 受信側の完了時に、L4パケットタイプの表示。
- 作業キュー用のCVLANインサートをサポート。

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterprise Server 11 SP4 (AMD64/EM64T)のカーネルは、次のとおりです。
3.0.101-63-default -(AMD64/EM64T)および将来のアップデートカーネル。
3.0.101-63-xen -(AMD64/EM64T)および将来のアップデートカーネル。

HPE Mellanox RoCE (RDMA over Converged Ethernet)ドライバー for SUSE LINUX Enterprise Server 11 SP3 (AMD64/EM64T)

バージョン: 4.3 **(推奨)**
ファイル名: 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

重要な注意！

Mellanox Ethernet + RoCE Linuxドライバー(mlnx-ofa_kernel RPM)は、HPE MellanoxアダプターのEthernet動作モードのみサポートします。完全なInfiniBand機能または"InfiniBand + Ethernet"動作モードを同じノード上で必要とする場

合、"Mellanox OFED VPI Drivers and Utilities"というLinuxソフトウェア配信リポジトリ(https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/)からMLNX-OFEDドライバーをインストールしてください。

修正

バージョン4.1で、以下の問題を解決しました。

- IPv6のプロシージャーが、基となるカーネルでサポートされていないときに呼び出されました。
- カーネル4.11で始まったメモリーリークの問題を修正し、将来のSKBリークの検出を容易にするために、Soft RoCEドライバーに警告メッセージを追加しました。
- RXeデバイスを仮想(ダミー)デバイスと組み合わせたときに、カーネルのクラッシュがしばしば発生していました。
- IPベースのGIDの損失が原因で、RoCE GIDキャッシュの競合状態がしばしば生じていました。
- 同じホスト上のクライアントとサーバー間のrdma_cm接続は、VLANインターフェイスを介して操作しているときは不可能でした。
- RDMACM接続の接続レートが高いときは、RDMA_CM_EVENT_UNREACHABLEというエラーメッセージが 表示されて失敗することがよくありました。
- ページサイズが16KBより大きいシステムでは、SR-IOV(シングルルートI/O仮想化)はサポートされていませんでした。

バージョン4.0で、以下の問題を解決しました。

- SLES12 SP2でドライバーの起動時にカーネルがメモリ不足になることがありました。
- MACアドレス00:00:00:00:00:00でスプーフィングチェックがオンになりました
- Large Receive Offload (LRO)がオンになっていたときにTCPパケットが不適切な方法で受信されました。
- RXリングサイズを大きくするとCQバッファーのメモリ割り当てが失敗することがよくありました。
- MLNX_ENドライバーが4KページのARMアーキテクチャーでロードに失敗しました。

以下の問題点がバージョン3.4で修正されました。

- もしmlx4_ibモジュールがロードされなかったとき、タイムアウト後の "ethtool" セルフテストが割り込みテストでしばしば失敗していました。
- まれな状況で、非同期のイベントハンドラーから呼ばれたmlx4_en_get_drvinfo() によって、システムリブートの間にカーネルパニックが発生することがありました。
- VF netdevsが開いている状態でSR-IOVを無効にしようとすると、操作が失敗しました。

以下の問題が、バージョン3.3 (A)　で修正されました。

- インターフェイスの名前を変更する際の "mlnx_interface_mgr.sh" スクリプトとudevフロー間の競合状態

以下の問題点がバージョン3.3で修正されました。

- SLES12 SP1でのドライバーロードの問題を修正するために互換性 ocrdma.koモジュールを追加しました。
- /sys/class/infiniband//ports// で発見されたエラーカウンターが、ConnectX-4 アダプターカード内で正しく機能しませんでした。
- TXキューカウンター形式を: xq_[tc]*[ring/channel]に変更しました。
- RDMA Sniffer機能の問題を修正しました。
- 仮想機能がethtoolファシリティで使用されている場合、エラーメッセージがログに出力されました。
- 物理リンクのダウン時、同じポート上での物理機能から、任意の仮想機能へのトラフィックが欠落していました。

バージョン3.2 (A) での修正:

- "infiniband support"グループにOS配布のRPMがすでにインストールされている場合、RoCEユーザースペースのライブラリであるRPM "mlnx-ofa_kernel"でインストールに失敗しました。
- 以前のバージョンのMLNX-ENドライバーがすでにインストールされている場合、RoCEドライバーアップグレードが正しく動作しません。これは、Mellanox Ethernet ポートが動作しない原因となります。

バージョン3.2での修正:

- もっとも近い NUMA ノードを、受信側スケーリング用のデフォルトに設定します。
- GROが有効になったときに、プロキシVXLANインターフェイスが正しく処理されないARP要求パケット。

拡張

HPE Mellanox RoCEドライバーv4.1は、以下の変更点および新機能を含みます。

- /sys/class/infiniband/mlx5_0/ports/1/hw_counters/ディレクトリの下にある追加のRoCE診断およびECN輻輳カウンターのサポート。
- rx-fcs ethtoolオフロード構成のサポート。通常、パケットのFCSは、アプリケーションソケットバッファー(skb)に送信される前にASICハードウェアによって切り捨てられます。Ethtoolを使用して、rx-fcsが切り捨てられないように設定しながら、分析のためにアプリケーションに渡すことができます。
- DSCP値に基づいてPFCを有効にするためのオプション。この解決方法を使用することで、VLANヘッダーの使用が必須ではなくなります。
- ECNパラメーターは次のディレクトリに移動されています。/sys/kernel/debug/mlx5//cc_params/
- mlx_fs_dump(ステアリングルールを読み出し可能な形式で出力するpythonツール)のサポート。
- 名前やIDなどのPCIピア属性を指定する際に、デバイスをオープンし、コンテキストを作成する機能。
- ハイパーバイザー上の検査済みVFを無効する機能。
- ローカルループバックが使用されていないときに、ローカルループバック(ユニキャストおよびマルチキャスト)をmlx5ドライバーによってデフォルトで無効にすることで、パフォーマンスを改善しました。mlx5ドライバーは、ユーザースペースのアプリケーションによって開いた伝送ドメインの数を記録します。複数のユーザースペースの伝送ドメインが開いている場合、ローカルループバックは自動的に有効になります。
- 1パルス/秒(1PPS)のサポート。これは、アダプターがアダプターカードの専用のピンで1パルス/秒を送受信できるようにする時刻同期機能です。
- シャットダウンおよびkexecフローでのドライバーの高速終了のサポート。
- NVMe over Fabrics (NVMEoF)オフロード(ハードウェアの新しいNVMEoF標準ターゲット(サーバー)側の実装)のサポート。
- デフォルトのRoCEモードを変更して、RDMA CMがRoCEv1ではなくRoCEv2で利用できるようにしました。クライアント側とサーバー側で同じRoCEモードをサポートするには、RDMA_CMセッションに両方の側が必要です。そうでない場合、クライアントはサーバーに接続できなくなります。

HPE Mellanox RoCEドライバーバージョン3.4は、以下の変更点および新機能を含みます。

- 以下のカーネルモジュールパラメーターを追加しました:
  - mlx4_en_only_mode
  - udev_dev_port_dev_id

HPE Mellanox RoCEドライバーv3.3は、以下の変更点および新機能を含みます。

- 修正のみ。

HPE Mellanox RoCEドライバーv3.2は、以下の変更点および新機能を含みます。

- ローパケットキューペアおよび作業キュー用のFCS分散。
- 受信側の完了時に、L4パケットタイプの表示。
- 作業キュー用のCVLANインサートをサポート。

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterprise Server 11 SP3 (AMD64/EM64T)のカーネルは、次のとおりです。
3.0.76-0.11-default -(AMD64/EM64T)および将来のアップデートカーネル。
3.0.76-0.11-xen -(AMD64/EM64T)および将来のアップデートカーネル。

HPE Mellanox RoCE (RDMA over Converged Ethernet)ドライバー for SUSE LINUX Enterprise Server 12 SP2 (AMD64/EM64T)

バージョン: 4.3 **(推奨)**
ファイル名: 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

重要な注意！

Mellanox Ethernet + RoCE Linuxドライバー(mlnx-ofa_kernel RPM)は、HPE MellanoxアダプターのEthernet動作モードのみサポートします。完全なInfiniBand機能または"InfiniBand + Ethernet"動作モードを同じノード上で必要とする場合、"Mellanox OFED VPI Drivers and Utilities"というLinuxソフトウェア配信リポジトリ(https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/)からMLNX-OFEDドライバーをインストールしてください。

修正

バージョン4.1で、以下の問題を解決しました。

- IPv6のプロシージャーが、基となるカーネルでサポートされていないときに呼び出されました。
- カーネル4.11で始まったメモリーリークの問題を修正し、将来のSKBリークの検出を容易にするために、Soft RoCEドライバーに警告メッセージを追加しました。
- RXeデバイスを仮想(ダミー)デバイスと組み合わせたときに、カーネルのクラッシュがしばしば発生していました。
- IPベースのGIDの損失が原因で、RoCE GIDキャッシュの競合状態がしばしば生じていました。
- 同じホスト上のクライアントとサーバー間のrdma_cm接続は、VLANインターフェイスを介して操作しているときは不可能でした。
- RDMACM接続の接続レートが高いときは、RDMA_CM_EVENT_UNREACHABLEというエラーメッセージが 表示されて失敗することがよくありました。
- ページサイズが16KBより大きいシステムでは、SR-IOV(シングルルートI/O仮想化)はサポートされていませんでした。

バージョン4.0で、以下の問題を解決しました。

- SLES12 SP2でドライバーの起動時にカーネルがメモリ不足になることがありました。
- MACアドレス00:00:00:00:00:00でスプーフィングチェックがオンになりました
- Large Receive Offload (LRO)がオンになっていたときにTCPパケットが不適切な方法で受信されました。
- RXリングサイズを大きくするとCQバッファーのメモリ割り当てが失敗することがよくありました。
- MLNX_ENドライバーが4KページのARMアーキテクチャーでロードに失敗しました。

以下の問題点がバージョン3.4で修正されました。

- もしmlx4_ibモジュールがロードされなかったとき、タイムアウト後の "ethtool" セルフテストが割り込みテストでしばしば失敗していました。
- まれな状況で、非同期のイベントハンドラーから呼ばれたmlx4_en_get_drvinfo() によって、システムリブートの間にカーネルパニックが発生することがありました。
- VF netdevsが開いている状態でSR-IOVを無効にしようとすると、操作が失敗しました。

以下の問題が、バージョン3.3 (A)　で修正されました。

- インターフェイスの名前を変更する際の "mlnx_interface_mgr.sh" スクリプトとudevフロー間の競合状態

以下の問題点がバージョン3.3で修正されました。

- SLES12 SP1でのドライバーロードの問題を修正するために互換性 ocrdma.koモジュールを追加しました。
- /sys/class/infiniband//ports// で発見されたエラーカウンターが、ConnectX-4 アダプターカード内で正しく機能しませんでした。
- TXキューカウンター形式を: xq_[tc]*[ring/channel]に変更しました。
- RDMA Sniffer機能の問題を修正しました。
- 仮想機能がethtoolファシリティで使用されている場合、エラーメッセージがログに出力されました。
- 物理リンクのダウン時、同じポート上での物理機能から、任意の仮想機能へのトラフィックが欠落していました。

バージョン3.2 (A) での修正:

- "infiniband support"グループにOS配布のRPMがすでにインストールされている場合、RoCEユーザースペースのライブラリであるRPM "mlnx-ofa_kernel"でインストールに失敗しました。
- 以前のバージョンのMLNX-ENドライバーがすでにインストールされている場合、RoCEドライバーアップグレードが正しく動作しません。これは、Mellanox Ethernet ポートが動作しない原因となります。

バージョン3.2での修正:

- もっとも近い NUMA ノードを、受信側スケーリング用のデフォルトに設定します。
- GROが有効になったときに、プロキシVXLANインターフェイスが正しく処理されないARP要求パケット。

拡張

HPE Mellanox RoCEドライバーv4.1は、以下の変更点および新機能を含みます。

- /sys/class/infiniband/mlx5_0/ports/1/hw_counters/ディレクトリの下にある追加のRoCE診断およびECN輻輳カウンターのサポート。
- rx-fcs ethtoolオフロード構成のサポート。通常、パケットのFCSは、アプリケーションソケットバッファー(skb)に送信される前にASICハードウェアによって切り捨てられます。Ethtoolを使用して、rx-fcsが切り捨てられないように設定しながら、分析のためにアプリケーションに渡すことができます。
- DSCP値に基づいてPFCを有効にするためのオプション。この解決方法を使用することで、VLANヘッダーの使用が必須ではなくなります。
- ECNパラメーターは次のディレクトリに移動されています。/sys/kernel/debug/mlx5//cc_params/
- mlx_fs_dump(ステアリングルールを読み出し可能な形式で出力するpythonツール)のサポート。
- 名前やIDなどのPCIピア属性を指定する際に、デバイスをオープンし、コンテキストを作成する機能。
- ハイパーバイザー上の検査済みVFを無効する機能。
- ローカルループバックが使用されていないときに、ローカルループバック(ユニキャストおよびマルチキャスト)をmlx5ドライバーによってデフォルトで無効にすることで、パフォーマンスを改善しました。mlx5ドライバーは、ユーザースペースのアプリケーションによって開いた伝送ドメインの数を記録します。複数のユーザースペースの伝送ドメインが開いている場合、ローカルループバックは自動的に有効になります。
- 1パルス/秒(1PPS)のサポート。これは、アダプターがアダプターカードの専用のピンで1パルス/秒を送受信できるようにする時刻同期機能です。
- シャットダウンおよびkexecフローでのドライバーの高速終了のサポート。
- NVMe over Fabrics (NVMEoF)オフロード(ハードウェアの新しいNVMEoF標準ターゲット(サーバー)側の実装)のサポート。
- デフォルトのRoCEモードを変更して、RDMA CMがRoCEv1ではなくRoCEv2で利用できるようにしました。クライアント側とサーバー側で同じRoCEモードをサポートするには、RDMA_CMセッションに両方の側が必要です。そうでない場合、クライアントはサーバーに接続できなくなります。

HPE Mellanox RoCEドライバーバージョン3.4は、以下の変更点および新機能を含みます。

- 以下のカーネルモジュールパラメーターを追加しました:
  - mlx4_en_only_mode
  - udev_dev_port_dev_id

HPE Mellanox RoCEドライバーv3.3は、以下の変更点および新機能を含みます。

- 修正のみ。

HPE Mellanox RoCEドライバーv3.2は、以下の変更点および新機能を含みます。

- ローパケットキューペアおよび作業キュー用のFCS分散。
- 受信側の完了時に、L4パケットタイプの表示。
- 作業キュー用のCVLANインサートをサポート。

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterprise Server 12 SP2 (AMD64/EM64T)のカーネルは、次のとおりです。
4.4.21-69-default - (AMD64/EM64T)および将来のアップデートカーネル。

HPE Mellanox RoCE (RDMA over Converged Ethernet)ドライバーfor Red Hat Enterprise Linux 7 Update 4 (x86_64)

バージョン: 4.3 **(推奨)**
ファイル名: 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

重要な注意！

Mellanox Ethernet + RoCE Linuxドライバー(mlnx-ofa_kernel RPM)は、HPE MellanoxアダプターのEthernet動作モードのみサポートします。完全なInfiniBand機能または"InfiniBand + Ethernet"動作モードを同じノード上で必要とする場合、"Mellanox OFED VPI Drivers and Utilities"というLinuxソフトウェア配信リポジトリ(https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/)からMLNX-OFEDドライバーをインストールしてください。

修正

バージョン4.1で、以下の問題を解決しました。

- IPv6のプロシージャーが、基となるカーネルでサポートされていないときに呼び出されました。
- カーネル4.11で始まったメモリーリークの問題を修正し、将来のSKBリークの検出を容易にするために、Soft RoCEドライバーに警告メッセージを追加しました。
- RXeデバイスを仮想(ダミー)デバイスと組み合わせたときに、カーネルのクラッシュがしばしば発生していました。
- IPベースのGIDの損失が原因で、RoCE GIDキャッシュの競合状態がしばしば生じていました。
- 同じホスト上のクライアントとサーバー間のrdma_cm接続は、VLANインターフェイスを介して操作しているときは不可能でした。
- RDMACM接続の接続レートが高いときは、RDMA_CM_EVENT_UNREACHABLEというエラーメッセージが 表示されて失敗することがよくありました。
- ページサイズが16KBより大きいシステムでは、SR-IOV(シングルルートI/O仮想化)はサポートされていませんでした。

バージョン4.0で、以下の問題を解決しました。

- SLES12 SP2でドライバーの起動時にカーネルがメモリ不足になることがありました。
- MACアドレス00:00:00:00:00:00でスプーフィングチェックがオンになりました
- Large Receive Offload (LRO)がオンになっていたときにTCPパケットが不適切な方法で受信されました。
- RXリングサイズを大きくするとCQバッファーのメモリ割り当てが失敗することがよくありました。
- MLNX_ENドライバーが4KページのARMアーキテクチャーでロードに失敗しました。

以下の問題点がバージョン3.4で修正されました。

- もしmlx4_ibモジュールがロードされなかったとき、タイムアウト後の "ethtool" セルフテストが割り込みテストでしばしば失敗していました。
- まれな状況で、非同期のイベントハンドラーから呼ばれたmlx4_en_get_drvinfo() によって、システムリブートの間にカーネルパニックが発生することがありました。
- VF netdevsが開いている状態でSR-IOVを無効にしようとすると、操作が失敗しました。

以下の問題が、バージョン3.3 (A)　で修正されました。

- インターフェイスの名前を変更する際の "mlnx_interface_mgr.sh" スクリプトとudevフロー間の競合状態

以下の問題点がバージョン3.3で修正されました。

- SLES12 SP1でのドライバーロードの問題を修正するために互換性 ocrdma.koモジュールを追加しました。
- /sys/class/infiniband//ports// で発見されたエラーカウンターが、ConnectX-4 アダプターカード内で正しく機能しませんでした。
- TXキューカウンター形式を: xq_[tc]*[ring/channel]に変更しました。
- RDMA Sniffer機能の問題を修正しました。
- 仮想機能がethtoolファシリティで使用されている場合、エラーメッセージがログに出力されました。
- 物理リンクのダウン時、同じポート上での物理機能から、任意の仮想機能へのトラフィックが欠落していました。

バージョン3.2 (A) での修正:

- "infiniband support"グループにOS配布のRPMがすでにインストールされている場合、RoCEユーザースペースのライブラリであるRPM "mlnx-ofa_kernel"でインストールに失敗しました。
- 以前のバージョンのMLNX-ENドライバーがすでにインストールされている場合、RoCEドライバーアップグレードが正しく動作しません。これは、Mellanox Ethernet ポートが動作しない原因となります。

バージョン3.2での修正:

- もっとも近い NUMA ノードを、受信側スケーリング用のデフォルトに設定します。
- GROが有効になったときに、プロキシVXLANインターフェイスが正しく処理されないARP要求パケット。

拡張

HPE Mellanox RoCEドライバーv4.1は、以下の変更点および新機能を含みます。

- /sys/class/infiniband/mlx5_0/ports/1/hw_counters/ディレクトリの下にある追加のRoCE診断およびECN輻輳カウンターのサポート。
- rx-fcs ethtoolオフロード構成のサポート。通常、パケットのFCSは、アプリケーションソケットバッファー(skb)に送信される前にASICハードウェアによって切り捨てられます。Ethtoolを使用して、rx-fcsが切り捨てられないように設定しながら、分析のためにアプリケーションに渡すことができます。
- DSCP値に基づいてPFCを有効にするためのオプション。この解決方法を使用することで、VLANヘッダーの使用が必須ではなくなります。
- ECNパラメーターは次のディレクトリに移動されています。/sys/kernel/debug/mlx5//cc_params/
- mlx_fs_dump(ステアリングルールを読み出し可能な形式で出力するpythonツール)のサポート。
- 名前やIDなどのPCIピア属性を指定する際に、デバイスをオープンし、コンテキストを作成する機能。
- ハイパーバイザー上の検査済みVFを無効する機能。
- ローカルループバックが使用されていないときに、ローカルループバック(ユニキャストおよびマルチキャスト)をmlx5ドライバーによってデフォルトで無効にすることで、パフォーマンスを改善しました。mlx5ドライバーは、ユーザースペースのアプリケーションによって開いた伝送ドメインの数を記録します。複数のユーザースペースの伝送ドメインが開いている場合、ローカルループバックは自動的に有効になります。
- 1パルス/秒(1PPS)のサポート。これは、アダプターがアダプターカードの専用のピンで1パルス/秒を送受信できるようにする時刻同期機能です。
- シャットダウンおよびkexecフローでのドライバーの高速終了のサポート。
- NVMe over Fabrics (NVMEoF)オフロード(ハードウェアの新しいNVMEoF標準ターゲット(サーバー)側の実装)のサポート。
- デフォルトのRoCEモードを変更して、RDMA CMがRoCEv1ではなくRoCEv2で利用できるようにしました。クライアント側とサーバー側で同じRoCEモードをサポートするには、RDMA_CMセッションに両方の側が必要です。そうでない場合、クライアントはサーバーに接続できなくなります。

HPE Mellanox RoCEドライバーバージョン3.4は、以下の変更点および新機能を含みます。

- 以下のカーネルモジュールパラメーターを追加しました:
  - mlx4_en_only_mode
  - udev_dev_port_dev_id

HPE Mellanox RoCEドライバーv3.3は、以下の変更点および新機能を含みます。

- 修正のみ。

HPE Mellanox RoCEドライバーv3.2は、以下の変更点および新機能を含みます。

- ローパケットキューペアおよび作業キュー用のFCS分散。
- 受信側の完了時に、L4パケットタイプの表示。
- 作業キュー用のCVLANインサートをサポート

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるRed Hat Enterprise Linux 7 Update 4 (x86_64)カーネルは、次の通りです。
3.10.0-693.el7 - (x86_64) および将来アップデートされるカーネル。

HPE Mellanox RoCE (RDMA over Converged Ethernet)ドライバーfor SUSE LINUX Enterprise Server 12 SP3 (AMD64/EM64T)

バージョン: 4.3 **(推奨)**
ファイル名: 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

重要な注意！

Mellanox Ethernet + RoCE Linuxドライバー(mlnx-ofa_kernel RPM)は、HPE MellanoxアダプターのEthernet動作モードのみサポートします。完全なInfiniBand機能または"InfiniBand + Ethernet"動作モードを同じノード上で必要とする場合、"Mellanox OFED VPI Drivers and Utilities"というLinuxソフトウェア配信リポジトリ(https://downloads.linux.hpe.com/SDR/project/mlnx_ofed/)からMLNX-OFEDドライバーをインストールしてください。

修正

バージョン4.1で、以下の問題を解決しました。

- IPv6のプロシージャーが、基となるカーネルでサポートされていないときに呼び出されました。
- カーネル4.11で始まったメモリーリークの問題を修正し、将来のSKBリークの検出を容易にするために、Soft RoCEドライバーに警告メッセージを追加しました。
- RXeデバイスを仮想(ダミー)デバイスと組み合わせたときに、カーネルのクラッシュがしばしば発生していました。
- IPベースのGIDの損失が原因で、RoCE GIDキャッシュの競合状態がしばしば生じていました。
- 同じホスト上のクライアントとサーバー間のrdma_cm接続は、VLANインターフェイスを介して操作しているときは不可能でした。
- RDMACM接続の接続レートが高いときは、RDMA_CM_EVENT_UNREACHABLEというエラーメッセージが 表示されて失敗することがよくありました。
- ページサイズが16KBより大きいシステムでは、SR-IOV(シングルルートI/O仮想化)はサポートされていませんでした。

バージョン4.0で、以下の問題を解決しました。

- SLES12 SP2でドライバーの起動時にカーネルがメモリ不足になることがありました。
- MACアドレス00:00:00:00:00:00でスプーフィングチェックがオンになりました
- Large Receive Offload (LRO)がオンになっていたときにTCPパケットが不適切な方法で受信されました。
- RXリングサイズを大きくするとCQバッファーのメモリ割り当てが失敗することがよくありました。
- MLNX_ENドライバーが4KページのARMアーキテクチャーでロードに失敗しました。

以下の問題点がバージョン3.4で修正されました。

- もしmlx4_ibモジュールがロードされなかったとき、タイムアウト後の "ethtool" セルフテストが割り込みテストでしばしば失敗していました。
- まれな状況で、非同期のイベントハンドラーから呼ばれたmlx4_en_get_drvinfo() によって、システムリブートの間にカーネルパニックが発生することがありました。
- VF netdevsが開いている状態でSR-IOVを無効にしようとすると、操作が失敗しました。

以下の問題が、バージョン3.3 (A)　で修正されました。

- インターフェイスの名前を変更する際の "mlnx_interface_mgr.sh" スクリプトとudevフロー間の競合状態

以下の問題点がバージョン3.3で修正されました。

- SLES12 SP1でのドライバーロードの問題を修正するために互換性 ocrdma.koモジュールを追加しました。
- /sys/class/infiniband//ports// で発見されたエラーカウンターが、ConnectX-4 アダプターカード内で正しく機能しませんでした。
- TXキューカウンター形式を: xq_[tc]*[ring/channel]に変更しました。
- RDMA Sniffer機能の問題を修正しました。
- 仮想機能がethtoolファシリティで使用されている場合、エラーメッセージがログに出力されました。
- 物理リンクのダウン時、同じポート上での物理機能から、任意の仮想機能へのトラフィックが欠落していました。

バージョン3.2 (A) での修正:

- "infiniband support"グループにOS配布のRPMがすでにインストールされている場合、RoCEユーザースペースのライブラリであるRPM "mlnx-ofa_kernel"でインストールに失敗しました。
- 以前のバージョンのMLNX-ENドライバーがすでにインストールされている場合、RoCEドライバーアップグレードが正しく動作しません。これは、Mellanox Ethernet ポートが動作しない原因となります。

バージョン3.2での修正:

- もっとも近い NUMA ノードを、受信側スケーリング用のデフォルトに設定します。
- GROが有効になったときに、プロキシVXLANインターフェイスが正しく処理されないARP要求パケット。

拡張

HPE Mellanox RoCEドライバーv4.1は、以下の変更点および新機能を含みます。

- /sys/class/infiniband/mlx5_0/ports/1/hw_counters/ディレクトリの下にある追加のRoCE診断およびECN輻輳カウンターのサポート。
- rx-fcs ethtoolオフロード構成のサポート。通常、パケットのFCSは、アプリケーションソケットバッファー(skb)に送信される前にASICハードウェアによって切り捨てられます。Ethtoolを使用して、rx-fcsが切り捨てられないように設定しながら、分析のためにアプリケーションに渡すことができます。
- DSCP値に基づいてPFCを有効にするためのオプション。この解決方法を使用することで、VLANヘッダーの使用が必須ではなくなります。
- ECNパラメーターは次のディレクトリに移動されています。/sys/kernel/debug/mlx5//cc_params/
- mlx_fs_dump(ステアリングルールを読み出し可能な形式で出力するpythonツール)のサポート。
- 名前やIDなどのPCIピア属性を指定する際に、デバイスをオープンし、コンテキストを作成する機能。
- ハイパーバイザー上の検査済みVFを無効する機能。
- ローカルループバックが使用されていないときに、ローカルループバック(ユニキャストおよびマルチキャスト)をmlx5ドライバーによってデフォルトで無効にすることで、パフォーマンスを改善しました。mlx5ドライバーは、ユーザースペースのアプリケーションによって開いた伝送ドメインの数を記録します。複数のユーザースペースの伝送ドメインが開いている場合、ローカルループバックは自動的に有効になります。
- 1パルス/秒(1PPS)のサポート。これは、アダプターがアダプターカードの専用のピンで1パルス/秒を送受信できるようにする時刻同期機能です。
- シャットダウンおよびkexecフローでのドライバーの高速終了のサポート。
- NVMe over Fabrics (NVMEoF)オフロード(ハードウェアの新しいNVMEoF標準ターゲット(サーバー)側の実装)のサポート。
- デフォルトのRoCEモードを変更して、RDMA CMがRoCEv1ではなくRoCEv2で利用できるようにしました。クライアント側とサーバー側で同じRoCEモードをサポートするには、RDMA_CMセッションに両方の側が必要です。そうでない場合、クライアントはサーバーに接続できなくなります。

HPE Mellanox RoCEドライバーバージョン3.4は、以下の変更点および新機能を含みます。

- 以下のカーネルモジュールパラメーターを追加しました:
  - mlx4_en_only_mode
  - udev_dev_port_dev_id

HPE Mellanox RoCEドライバーv3.3は、以下の変更点および新機能を含みます。

- 修正のみ。

HPE Mellanox RoCEドライバーv3.2は、以下の変更点および新機能を含みます。

- ローパケットキューペアおよび作業キュー用のFCS分散。
- 受信側の完了時に、L4パケットタイプの表示。
- 作業キュー用のCVLANインサートをサポート。

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterprise Server 12 SP3 (AMD64/EM64T)のカーネルは、次のとおりです。
4.4.73-5-default -(AMD64/EM64T)および将来のアップデートカーネル。

HPE QLogic FastLinQ 10/25/50 GbEマルチファンクションドライバーfor VMware vSphere 6.0

バージョン: 2018.06.04 **(オプション)**
ファイル名: cp033819.compsig; cp033819.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCP0xxxxx.xmlファイルから利用可能な同じドライバーを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE QLogic FastLinQ Online Firmware Upgrade Utility for VMware*、バージョン4.6.24以降で提供されるファームウェアを推奨しています。

修正

この製品は、システムが再起動中にハングする問題を解決します。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic FastLinQ 10/25/50 GbEマルチファンクションドライバーfor VMware vSphere 6.5

バージョン: 2018.06.04 **(オプション)**
ファイル名: cp033820.compsig; cp033820.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCP0xxxxx.xmlファイルから利用可能な同じドライバーを含むzipファイルです。

このドライバーとともに使用する場合は、*HPE QLogic FastLinQ Online Firmware Upgrade Utility for VMware*、バージョン4.6.24以降で提供されるファームウェアを推奨しています。

修正

この製品は、システムが再起動中にハングする問題を解決します。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic iSCSI Offload IO Daemon for Red Hat Enterprise Linux 6 Update 8 x86_64

バージョン: 2.11.5.5-6 **(オプション)**
ファイル名: iscsiuio-2.11.5.5-6.rhel6u8.x86_64.compsig; iscsiuio-2.11.5.5-6.rhel6u8.x86_64.rpm; README

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP FlexFabric 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic iSCSI Offload IO Daemon for Red Hat Enterprise Linux 6 Update 9 x86_64

バージョン: 2.11.5.5-6 **(オプション)**

ファイル名: iscsiuio-2.11.5.5-6.rhel6u9.x86_64.compsig; iscsiuio-2.11.5.5-6.rhel6u9.x86_64.rpm; README

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP FlexFabric 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic iSCSI Offload IO Daemon for Red Hat Enterprise Linux 7 Update 4 x86_64

バージョン: 2.11.5.5-6 **(オプション)**

ファイル名: iscsiuio-2.11.5.5-6.rhel7u4.x86_64.compsig; iscsiuio-2.11.5.5-6.rhel7u4.x86_64.rpm; README

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター

- HP FlexFabric 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic iSCSI Offload IO Daemon for Red Hat Enterprise Linux 7 Update 5 x86_64

バージョン: 2.11.5.5-6 **(オプション)**
ファイル名: iscsiuio-2.11.5.5-6.rhel7u5.x86_64.compsig; iscsiuio-2.11.5.5-6.rhel7u5.x86_64.rpm; README

拡張

Initial release.

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP FlexFabric 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic iSCSI Offload IO Daemon for SUSE Linux Enterprise Server 11 SP3 x86_64

バージョン: 2.11.5.5-6 **(オプション)**
ファイル名: iscsiuio-2.11.5.5-6.sles11sp3.x86_64.compsig; iscsiuio-2.11.5.5-6.sles11sp3.x86_64.rpm; README

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HP Ethernet 10Gb 2ポート 530SFP+アダプター

- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP FlexFabric 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic iSCSI Offload IO Daemon for SUSE Linux Enterprise Server 11 SP4 x86_64

バージョン: 2.11.5.5-6 **(オプション)**
ファイル名: iscsiuio-2.11.5.5-6.sles11sp4.x86_64.compsig; iscsiuio-2.11.5.5-6.sles11sp4.x86_64.rpm; README

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP FlexFabric 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic iSCSI Offload IO Daemon for SUSE Linux Enterprise Server 12 SP2 x86_64

バージョン: 2.11.5.5-6 **(オプション)**
ファイル名: iscsiuio-2.11.5.5-6.sles12sp2.x86_64.compsig; iscsiuio-2.11.5.5-6.sles12sp2.x86_64.rpm; README

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP FlexFabric 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター

- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic iSCSI Offload IO Daemon for SUSE Linux Enterprise Server 12 SP3 x86_64

バージョン: 2.11.5.5-6 **(オプション)**
ファイル名: iscsiuio-2.11.5.5-6.sles12sp3.x86_64.compsig; iscsiuio-2.11.5.5-6.sles12sp3.x86_64.rpm; README

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP FlexFabric 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic NX2 10/20 GbE マルチファンクションドライバーfor Windows Server x64 Editions

バージョン: 7.13.145.0 **(オプション)**
ファイル名: cp034362.compsig; cp034362.exe

重要な注意！

これらのドライバーとともに使用する場合は、*HPE QLogic NX2 Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP Ethernet 10Gb 2ポート 533FLR-Tアダプター

- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 10Gb 2820C Ethernetアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

HPE QLogic NX2 10/20 GbEマルチファンクションドライバーfor Red Hat Enterprise Linux 6 x86_64

バージョン: 7.14.48-1 **(オプション)**
ファイル名: kmod-netxtreme2-7.14.48-1.rhel6u8.x86_64.compsig; kmod-netxtreme2-7.14.48-1.rhel6u8.x86_64.rpm; kmod-netxtreme2-7.14.48-1.rhel6u9.x86_64.compsig; kmod-netxtreme2-7.14.48-1.rhel6u9.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE QLogic NX2 Online Firmware Upgrade Utility for Linux x86_64*、バージョン2.22.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP Ethernet 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

HPE QLogic NX2 10/20 GbEマルチファンクションドライバーfor Red Hat Enterprise Linux 7 x86_64

バージョン: 7.14.48-1 **(オプション)**
ファイル名: kmod-netxtreme2-7.14.48-1.rhel7u4.x86_64.compsig; kmod-netxtreme2-7.14.48-1.rhel7u4.x86_64.rpm; kmod-netxtreme2-7.14.48-1.rhel7u5.x86_64.compsig; kmod-netxtreme2-7.14.48-1.rhel7u5.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE QLogic NX2 Online Firmware Upgrade Utility for Linux x86_64*、バージョン2.22.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 530SFP+アダプター

- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP Ethernet 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

HPE QLogic NX2 10/20 GbEマルチファンクションドライバーfor SUSE Linux Enterprise Server 11 x86_64

バージョン: 7.14.48-2 **(オプション)**
ファイル名: netxtreme2-kmp-default-7.14.48_3.0.101_63-1.sles11sp4.x86_64.compsig; netxtreme2-kmp-default-7.14.48_3.0.101_63-1.sles11sp4.x86_64.rpm; netxtreme2-kmp-default-7.14.48_3.0.76_0.11-2.sles11sp3.x86_64.compsig; netxtreme2-kmp-default-7.14.48_3.0.76_0.11-2.sles11sp3.x86_64.rpm; netxtreme2-kmp-xen-7.14.48_3.0.101_63-1.sles11sp4.x86_64.compsig; netxtreme2-kmp-xen-7.14.48_3.0.101_63-1.sles11sp4.x86_64.rpm; netxtreme2-kmp-xen-7.14.48_3.0.76_0.11-2.sles11sp3.x86_64.compsig; netxtreme2-kmp-xen-7.14.48_3.0.76_0.11-2.sles11sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE QLogic NX2 Online Firmware Upgrade Utility for Linux x86_64*、バージョン2.22.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP Ethernet 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

HPE QLogic NX2 10/20 GbEマルチファンクションドライバーfor SUSE Linux Enterprise Server 12 x86_64

バージョン: 7.14.46-1 **(オプション)**
ファイル名: 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

重要な注意！

これらのドライバーとともに使用する場合は、*HPE QLogic NX2 Online Firmware Upgrade Utility for Linux x86_64*、バージョン2.22.15以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP Ethernet 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

HPE QLogic NX2 10/20 GbEマルチファンクションドライバーfor SUSE Linux Enterprise Server 12 x86_64

バージョン: 7.14.48-1 **(オプション)**
ファイル名: netxtreme2-kmp-default-7.14.48_k4.4.21_69-1.sles12sp2.x86_64.compsig; netxtreme2-kmp-default-7.14.48_k4.4.21_69-1.sles12sp2.x86_64.rpm; netxtreme2-kmp-default-7.14.48_k4.4.73_5-1.sles12sp3.x86_64.compsig; netxtreme2-kmp-default-7.14.48_k4.4.73_5-1.sles12sp3.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE QLogic NX2 Online Firmware Upgrade Utility for Linux x86_64*、バージョン2.22.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP Ethernet 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

---

net-mstカーネルモジュールドライバーコンポーネント for VMware 6.0

バージョン: 2018.01.22 **(推奨)**
ファイル名: cp034694.compsig; cp034694.zip
ドライバー名およびバージョン:

修正

NMSTバージョン4.9.0.38

拡張

NMSTバージョン4.9.0.38

---

net-mstカーネルモジュールドライバーコンポーネント for VMware 6.5

バージョン: 2018.01.22 **(推奨)**
ファイル名: cp034695.compsig; cp034695.zip
ドライバー名およびバージョン:

修正

NMSTバージョン 4.9.0.38

拡張

NMSTバージョン 4.9.0.38

---

nmlx4_enドライバーコンポーネント for VMware 6.0

バージョン: 2018.03.13 **(推奨)**
ファイル名: cp035374.zip; cp035374_part1.compsig; cp035374_part2.compsig
ドライバー名およびバージョン:

修正

修正:

- RX および TX内でVLAN タグ Priority Code Point (PCP) が正しく動作しない問題を修正しました。
- RDMA モジュールが削除されなかった場合のインストレーション中のPSOD ケースを修正しました。
- マネジメントインターフェイスポートタイプフィールド (nmlx-_en_MgmtIFPortType)が誤った値を報告しました。

---

nmlx4_enドライバーコンポーネント for VMware 6.5

バージョン: 2018.03.13 **(推奨)**
ファイル名: cp035375.zip; cp035375_part1.compsig; cp035375_part2.compsig; cp035375_part3.compsig
ドライバー名およびバージョン:

拡張

3.15.5.5の変更内容:

- VXLANハードウェアオフロードのサポートを追加しました。 VXLAN ハードウェアオフロードは従来型のオフロードが、カプセル化されたトラフィックで実行するのを可能にします。 ConnectX®-3 Proでは、データセンターのオペレーターが物理NICパフォーマンスからオーバーレイネットワークレイヤーを切り離すことができるため、新しいネットワークアーキテクチーでネイティブパフォーマンスを達成できるようになります。
- 管理インターフェイスのサポートを追加しました。
- **ハードウェアパフォーマンス**
  - 1G
  - 10G
  - 40G
- Large Send Offload(TCPセグメンテーションオフロード)
- WoL(サポートされているハードウェア上でのみ)
- RSSキュー

- 複数Tx/Rxリング
- NetQueueのサポート
- パススルーを修正
- シングル/デュアルポート
- MSI-X

---

nmlx5_enドライバーコンポーネント for VMware 6.0

バージョン: 2018.01.22 **(推奨)**
ファイル名: cp034603.compsig; cp034603.zip
ドライバー名およびバージョン:

修正

修正:

- ESXi5.5で – ConnectX-4 / ConnectX-4 Lxポートが多いサーバーを使用している場合、一部のインターフェイスがesxcfg-nics -lリストに表示されません。これは、すべてのインターフェイスをロードするためのMSI-Xリソールがない場合に発生します。
- SR-IOVが有効でmax_vfsが0でない場合、新しいフィルターが適用されません。
- "8" のConnectX-4のLxポートまでサポートする "supported_ num_ports" をnmlx5_coreに新しいモジュールパラメーターが追加されました。
- 64以上のCPUコア搭載のマシン上でドライバーをロードすることを妨げる問題を修正しました。

---

nmlx5_enドライバーコンポーネント for VMware 6.5

バージョン: 2018.01.22 **(推奨)**
ファイル名: cp034604.zip; cp034604_part1.compsig; cp034604_part2.compsig
ドライバー名およびバージョン:

修正

4.16.8.8での修正:

- リングサイズを8192に設定した後、アダプターカードがダウン状態から動けなくなる問題を修正しました。

拡張

バージョン4.16.8.8の新機能および変更:

- ConnectX-5/ConnectX-5 Exアダプターカードのサポートを追加しました。
  注:ConnectX-5/ConnectX-5 Exカードは現在ベータレベルです。

Red Hat Enterprise Linux 6 x86_64用HPE Intel i40eドライバー

バージョン: 2.4.6.1-7 **(推奨)**
ファイル名: kmod-hp-i40e-2.4.6.1-7.rhel6u8.x86_64.compsig; kmod-hp-i40e-2.4.6.1-7.rhel6u8.x86_64.rpm; kmod-hp-i40e-2.4.6.1-7.rhel6u9.x86_64.compsig; kmod-hp-i40e-2.4.6.1-7.rhel6u9.x86_64.rpm; README

重要な注意！

これらのドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.15.56以降で提供されるファームウェアを推奨しています。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 1Gb 2ポート 368i アダプター

- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2ポート 563i アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター

Red Hat Enterprise Linux 6 x86_64用HPE QLogic FastLinQ 10/25/50 GbEドライバー

バージョン: 8.33.17.0-1 **(オプション)**
ファイル名: 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

重要な注意！

これらドライバーとともに使用する場合は、*HPE QLogic FastLinQ Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.4.24以降で提供されるファームウェアを推奨しています。

修正

この製品は、機能がまだプロービングされている間にMFWがプロトコル統計情報を呼び出したときに見られるシステムクラッシュを修正します。
この製品は、LL2バッファサイズの制限を設定する際に発生する問題を修正します。

拡張

この製品は現在、パケットフィルター[パケットペーシング]の最大転送レート設定をサポートしています。
この製品は現在、Macvlanオフロードをサポートします。
この製品は現在、ポート統計情報の中の'link_change_count'をサポートします。
この製品は現在、モジュール paramによって LL2 バッファまたは pingパケットのサイズの設定をサポートします。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

Red Hat Enterprise Linux 6アップデート8向けHPE QLogic FastLinQ RoCEライブラリ

バージョン: 8.33.1.0-1 **(オプション)**
ファイル名: qlgc-libqedr-8.33.1.0-1.rhel6u8.x86_64.compsig; qlgc-libqedr-8.33.1.0-1.rhel6u8.x86_64.rpm; README

事前要件

この製品をインストールする前に、*HPE QLogic FastLinQ 10/25/50GbE Drivers for Red Hat Enterprise Linux 6 x86_64*、バージョン8.33.17.0-1以降をインストールする必要があります。

RoCEライブラリをインストールする前に、ターゲットシステムにlibibverbパッケージをインストールしておく必要があります。まだインストールしていない場合は、オペレーティングシステムのインストールメディアからlibibverbパッケージを取得できます。

修正

この製品は、レガシーData Protection Manager (DPM)を使用しているときに見られるrstreamアプリケーションのハングを修正します。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

Red Hat Enterprise Linux 6アップデート9向けHPE QLogic FastLinQ RoCEライブラリ

バージョン: 8.33.1.0-1 **(オプション)**
ファイル名: qlgc-libqedr-8.33.1.0-1.rhel6u9.x86_64.compsig; qlgc-libqedr-8.33.1.0-1.rhel6u9.x86_64.rpm; README

事前要件

この製品をインストールする前に、*HPE QLogic FastLinQ 10/25/50GbE Drivers for Red Hat Enterprise Linux 6 x86_64*、バージョン8.33.17.0-1以降をインストールする必要があります。

RoCEライブラリをインストールする前に、ターゲットシステムにlibibverbパッケージをインストールしておく必要があります。まだインストールしていない場合は、オペレーティングシステムのインストールメディアからlibibverbパッケージを取得できます。

修正

この製品は、レガシーData Protection Manager (DPM)を使用しているときに見られるrstreamアプリケーションのハングを修正します。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

Red Hat Enterprise Linux 6アップデート9用HPE Broadcom NetXtreme-E RoCEライブラリ

バージョン: 212.0.82.0 (B) **(推奨)**
ファイル名: libbnxtre-212.0.82.0-rhel6u9.x86_64.compsig; libbnxtre-212.0.82.0-rhel6u9.x86_64.rpm; README

事前要件

この製品をインストールする前に、*HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6*、バージョン1.9.1-212.0.99.0以降をインストールする必要があります。

RoCEライブラリをインストールする前に、ターゲットシステムにlibibverbパッケージをインストールしておく必要があります。まだインストールしていない場合は、オペレーティングシステムのインストールメディアからlibibverbパッケージを取得できます。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

Red Hat Enterprise Linux 7 x86_64用HPE QLogic FastLinQ 10/25/50 GbEドライバー

バージョン: 8.33.17.0-1 **(オプション)**
ファイル名: 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

重要な注意！

これらドライバーとともに使用する場合は、*HPE QLogic FastLinQ Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.4.24以降で提供されるファームウェアを推奨しています。

修正

この製品は、機能がまだプロービングされている間にMFWがプロトコル統計情報を呼び出したときに見られるシステムクラッシュを修正します。
この製品は、LL2バッファサイズの制限を設定する際に発生する問題を修正します。

拡張

この製品は現在、パケットフィルター[パケットペーシング]の最大転送レート設定をサポートしています。
この製品は現在、Macvlanオフロードをサポートします。
この製品は現在、ポート統計情報の中の'link_change_count'をサポートします。
この製品は現在、モジュール paramによって LL2 バッファまたは pingパケットのサイズの設定をサポートします。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

Red Hat Enterprise Linux 7アップデート4用HPE Broadcom NetXtreme-E RoCEライブラリ

バージョン: 212.0.82.0 (B) **(推奨)**
ファイル名: libbnxt_re-212.0.82.0-rhel7u4.x86_64.compsig; libbnxt_re-212.0.82.0-rhel7u4.x86_64.rpm; README

事前要件

この製品をインストールする前に、*HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6*、バージョン1.9.1-212.0.99.0以降をインストールする必要があります。

RoCEライブラリをインストールする前に、ターゲットシステムにlibibverbパッケージをインストールしておく必要があります。まだインストールしていない場合は、オペレーティングシステムのインストールメディアからlibibverbパッケージを取得できます。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

SUSE Linux Enterprise Server 11 SP4向けHPE QLogic FastLinQ RoCEライブラリ

バージョン: 8.33.1.0-1 **(オプション)**
ファイル名: qlgc-libqedr-8.33.1.0-1.sles11sp4.x86_64.compsig; qlgc-libqedr-8.33.1.0-1.sles11sp4.x86_64.rpm; README

事前要件

この製品をインストールする前に、*HPE QLogic FastLinQ 10/25/50GbE Drivers for SUSE Linux Enterprise Server 11 x86_64*、バージョン8.33.17.0-1以降をインストールする必要があります。

RoCEライブラリをインストールする前に、ターゲットシステムにlibibverbパッケージをインストールしておく必要があります。まだインストールしていない場合は、オペレーティングシステムのインストールメディアからlibibverbパッケージを取得できます。

修正

この製品は、レガシーData Protection Manager (DPM)を使用しているときに見られるrstreamアプリケーションのハングを修正します。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

SUSE Linux Enterprise Server 11 SP4用HPE Broadcom NetXtreme-E RoCEライブラリ

バージョン: 212.0.82.0 (B) **(推奨)**
ファイル名: libbnxtre-212.0.82.0-sles11sp4.x86_64.compsig; libbnxtre-212.0.82.0-sles11sp4.x86_64.rpm; README

事前要件

この製品をインストールする前に、*HPE Broadcom NetXtreme-E Drivers for Red Hat Enterprise Linux 6*、バージョン1.9.1-212.0.99.0以降をインストールする必要があります。

RoCEライブラリをインストールする前に、ターゲットシステムにlibibverbパッケージをインストールしておく必要があります。まだインストールしていない場合は、オペレーティングシステムのインストールメディアからlibibverbパッケージを取得できます。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター

- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

SUSE Linux Enterprise Server 11 x86_64用HPE QLogic FastLinQ 10/25/50 GbEドライバー

バージョン: 8.33.17.0-1 **(オプション)**
ファイル名: 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

重要な注意！

これらドライバーとともに使用する場合は、*HPE QLogic FastLinQ Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.4.24以降で提供されるファームウェアを推奨しています。

修正

この製品は、機能がまだプロービングされている間にMFWがプロトコル統計情報を呼び出したときに見られるシステムクラッシュを修正します。
この製品は、LL2バッファサイズの制限を設定する際に発生する問題を修正します。

拡張

この製品は現在、パケットフィルター[パケットペーシング]の最大転送レート設定をサポートしています。
この製品は現在、Macvlanオフロードをサポートします。
この製品は現在、ポート統計情報の中の'link_change_count'をサポートします。
この製品は現在、モジュール paramによって LL2 バッファまたは pingパケットのサイズの設定をサポートします。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

SUSE Linux Enterprise Server 12 SP2向けHPE QLogic FastLinQ RoCEライブラリ

バージョン: 8.33.1.0-1 **(オプション)**
ファイル名: qlgc-libqedr-8.33.1.0-1.sles12sp2.x86_64.compsig; qlgc-libqedr-8.33.1.0-1.sles12sp2.x86_64.rpm; README

事前要件

この製品をインストールする前に、*HPE QLogic FastLinQ 10/25/50GbE Drivers for SUSE Linux Enterprise Server 12 x86_64*、バージョン8.33.17.0-1以降をインストールする必要があります。

RoCEライブラリをインストールする前に、ターゲットシステムにlibibverbパッケージをインストールしておく必要があります。まだインストールしていない場合は、オペレーティングシステムのインストールメディアからlibibverbパッケージを取得できます。

修正

この製品は、レガシーData Protection Manager (DPM)を使用しているときに見られるrstreamアプリケーションのハングを修正します。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

SUSE Linux Enterprise Server 12 x86_64用HPE QLogic FastLinQ 10/25/50 GbEドライバー

バージョン: 8.33.17.0-1 **(オプション)**
ファイル名: 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

重要な注意！

これらドライバーとともに使用する場合は、*HPE QLogic FastLinQ Online Firmware Upgrade Utility for Linux x86_64*、バージョン1.4.24以降で提供されるファームウェアを推奨しています。

修正

この製品は、機能がまだプロービングされている間にMFWがプロトコル統計情報を呼び出したときに見られるシステムクラッシュを修正します。
この製品は、LL2バッファサイズの制限を設定する際に発生する問題を修正します。

拡張

この製品は現在、パケットフィルター[パケットペーシング]の最大転送レート設定をサポートしています。
この製品は現在、Macvlanオフロードをサポートします。
この製品は現在、ポート統計情報の中の'link_change_count'をサポートします。
この製品は現在、モジュール paramによって LL2 バッファまたは pingパケットのサイズの設定をサポートします。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

VMware ESX 6.0 MSTドライバー オフラインバンドル for Mellanoxアダプター

バージョン: 4.9.0.38 **(推奨)**
ファイル名: MLNX-NMST-ESX-6.0.0-4.9.0.38.zip

拡張

VM60 nmst 4.8.0.200

VMware ESX 6.5 MSTドライバー オフラインバンドル for Mellanoxアダプター

バージョン: 4.9.0.38 **(推奨)**
ファイル名: MLNX-NMST-ESX-6.5.0-4.9.0.38.zip

拡張

VM65 nmst 4.8.0.200

VMware vSphere 6.0用HPE QLogic NX2 10/20 GbEマルチファンクションドライバー

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035304.compsig; cp035304.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCP0xxxxx.xmlファイルから利用可能な同じドライバーを含むzipファイルです。

HPEは、このドライバーでの使用に、*HPE QLogic NX2*オンラインファームウェアアップグレードユーティリティ *for VMware*、バージョン1.22.2で提供されるファームウェアをおすすめします。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP Ethernet 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- 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コンバージドネットワークアダプター

VMware vSphere 6.5用HPE QLogic NX2 10/20 GbEマルチファンクションドライバー

バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035302.compsig; cp035302.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCP0xxxxx.xmlファイルから利用可能な同じドライバーを含むzipファイルです。

HPEは、このドライバーでの使用に、*HPE QLogic NX2*オンラインファームウェアアップグレードユーティリティ *for VMware*、バージョン1.22.2で提供されるファームウェアをおすすめします。

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP Ethernet 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター

- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T デュアルポートコンバージドネットワークアダプター
- HPE Synergy 10Gb 2ポート 2820C コンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

Windows Server 2012用HPE Intel v40eドライバー

バージョン: 1.5.65.0 (B) **(オプション)**
ファイル名: cp034521.compsig; cp034521.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

事前要件

このドライバーではホストドライバーバージョン1.8.90.0以降が必要です。

サポートしているデバイスおよび機能

この製品は、以下のHPE Intel i40eaネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター

Windows Server 2016用HPE Intel ixsドライバー

バージョン: 4.1.74.0 **(オプション)**
ファイル名: cp033710.compsig; cp033710.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.2.2以降で提供されるファームウェアを推奨しています。

拡張

このドライバーは、最新のNDISドライバーとの互換性を維持するためにアップデートされています。

サポートしているデバイスおよび機能

このドライバーは、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター

Windows Server 2016用HPE Intel v40eドライバー

バージョン: 1.5.76.0 **(オプション)**
ファイル名: cp034523.compsig; cp034523.exe

重要な注意！

このドライバーとともに使用する場合は、*HPE Intel Online Firmware Upgrade Utility for Windows Server x64 Edition*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

事前要件

このドライバーではホストドライバーバージョン1.8.90.0以降が必要です。

サポートしているデバイスおよび機能

この製品は、以下のHPE Intel i40eaネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター

Windows Server x64 Edition用HPE QLogic FastLinQ 10/25/50 GbEドライバー

バージョン: 8.33.23.0 **(オプション)**
ファイル名: cp033844.compsig; cp033844.exe

重要な注意！

これらのドライバーとともに使用する場合は、*HPE QLogic FastLinQ*オンラインファームウェアアップグレードユーティリティ*for Windows Server x64 Editions*、バージョン5.1.3.0以降で提供されるファームウェアを推奨しています。

修正

- このドライバーは、RDMAモードのときにデバイスマネージャの詳細プロパティの下にiWARPが表示されないという問題に対処します。
- このドライバーは、リンク速度が常に10Gbpsであることが表示されている問題に対処します。
- このドライバーは、iWARPトラフィックを実行した後、NIC拡張パラメーターを変更したときに表示されるシステムクラッシュに対処します。
- このドライバーは、VBDドライバーにRoCEトラフィックをロードまたはアンロードする際に表示されるシステムクラッシュに対処します。
- このドライバーは、Virtual Switch RSSパラメーターが無効になっているときに表示されるシステムクラッシュに対処します。
- このドライバーは、ゲストドライバーが構成された仮想マシンキューでトラフィックを実行しているときに、再起動時に表示されるシステムクラッシュに対処します。
- このドライバーは、アダプターポートからIPv6バインディングを無効にするときに見られるシステムクラッシュに対処します。
- このドライバーは、ドライバの検証とミニポートを無効にするときに見られるシステムクラッシュに対処します。
- このドライバーは、プロセッサーグループが異なる場合に異なったNUMAノード間でRSSプロセッサーの選択が行われない問題を修正します。
- このドライバーは、予期しないL2トラフィックを受信した場合の問題を修正します。
- このドライバーは、iWARP受信ウィンドウサイズの最大範囲の不一致を修正します。
- このドライバーは、ホストDCB設定がNon-Willingモードのアダプターで有効にならない問題を修正します。

拡張

RDMAキューペア(QPs)の最大数を4096に増加しました。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター

- HPE Synergy 6810C 25/50Gb Ethernetアダプター

ドライバー - セキュリティ

先頭

AMD Secure Processorドライバー for Windows Server 2012 R2

バージョン: 4.1.0.0 (C) **(オプション)**
ファイル名: cp034066.compsig; cp034066.exe

拡張

HPE ProLiant DL325 Gen10のサポートを追加しました。

AMD Secure Processorドライバー for Windows Server 2016

バージョン: 4.1.0.0 (C) **(オプション)**
ファイル名: cp034067.compsig; cp034067.exe

拡張

HPE ProLiant DL325 Gen10のサポートを追加しました。

ドライバー - ストレージ

先頭

Dynamic SmartアレイP741m B140iコントローラードライバーfor 64ビットMicrosoft Windows Server 2012/2016 Editions

バージョン: 62.12.0.64 **(推奨)**
ファイル名: cp028631.exe

拡張

不必要なメッセージをフィルターで取り除き、重要なデータのみを保持するために光学デバイスからのデバッグ出力を削減します。

Microsoft Windows Server 2016のサポートを追加しました。

HPE SmartアレイS100i SR Gen10 SW RAIDドライバーfor Windows Server 2012 R2および Windows Server 2016

バージョン: 100.8.0.0 **(推奨)**
ファイル名: cp036395.compsig; cp036395.exe

修正

ドライブ交換などのメディア交換イベントの後、システムの再起動時に、初期化されていない変数がRAIDスタックコードに存在すると、安定したRAIDボリュームが故障する可能性があります。この問題は、Windows SmartDQドライバーのバージョン100.8.0.0で解決されています。

ドライバー - ストレージコントローラー

先頭

64-bit Red Hat Enterprise Linux 6用HPE SmartアレイP824i-p MRコントローラードライバー

バージョン: 07.702.10.00-11 **(推奨)**
ファイル名: kmod-megaraid_sas-07.702.10.00-11.rhel6u9.x86_64.compsig; kmod-megaraid_sas-07.702.10.00-

11.rhel6u9.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるRed Hat Enterprise Linux 6 (64-bit)カーネルは、次の通りです。

2.6.32-696.el6 - Red Hat Enterprise Linux 6 Update 9(64-bit)およびfuture errata kernels for update 9。

64-bit Red Hat Enterprise Linux 7用HPE SmartアレイP824i-p MRコントローラードライバー

バージョン: 07.702.10.00-11 **(推奨)**
ファイル名: kmod-megaraid_sas-07.702.10.00-11.rhel7u3.x86_64.compsig; kmod-megaraid_sas-07.702.10.00-11.rhel7u3.x86_64.rpm; kmod-megaraid_sas-07.702.10.00-11.rhel7u4.x86_64.compsig; kmod-megaraid_sas-07.702.10.00-11.rhel7u4.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるRed Hat Enterprise Linux 7 (64-bit)カーネルは、次のとおりです。
3.10.0-514.el7- Red Hat Enterprise Linux 7 Update 3(64-bit)および future errata kernels for update 3。
3.10.0-693.el7 - Red Hat Enterprise Linux 7 Update 4 (64-bit)およびfuture errata kernels for update 4。

64-bit SUSE LINUX Enterprise Server 11用HPE Smartアレイ P824i-p MRコントローラードライバー

バージョン: 07.702.10.00-11 **(推奨)**
ファイル名: lsi-megaraid_sas-kmp-default-07.702.10.00-11.sles11sp4.x86_64.compsig; lsi-megaraid_sas-kmp-default-07.702.10.00-11.sles11sp4.x86_64.rpm; lsi-megaraid_sas-kmp-xen-07.702.10.00-11.sles11sp4.x86_64.compsig; lsi-megaraid_sas-kmp-xen-07.702.10.00-11.sles11sp4.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このドライバーディスケットでサポートされるSUSE LINUX Enterpriseサーバー 11 (64-bit)カーネルは、次のとおりです。
3.0.101-63-デフォルト - SUSE LINUX Enterpriseサーバー11 SP 4 (64-bit) plus future errata。

64-bit SUSE LINUX Enterprise Server 12用HPE SmartアレイP824i-p MRコントローラードライバー

バージョン: 07.702.09.00-11 **(推奨)**
ファイル名: 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

修正

HPE SmartアレイPクラスMR Gen10コントローラーの初期ドライバーリリース。

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterpriseサーバー 12 (64-bit)カーネルは、次のとおりです。
4.4.21-69-default - SUSE LINUX Enterpriseサーバー12 (64-bit) SP2 plus future errata。
4.4.73-5.1 - SUSE LINUX Enterpriseサーバー12 (64-bit) SP3 plus future errata。

64-bit SUSE LINUX Enterprise Server 12用HPE SmartアレイP824i-p MRコントローラードライバー

バージョン: 07.702.10.00-11 **(推奨)**
ファイル名: lsi-megaraid_sas-kmp-default-07.702.10.00-11.sles12sp2.x86_64.compsig; lsi-megaraid_sas-kmp-default-07.702.10.00-11.sles12sp2.x86_64.rpm; lsi-megaraid_sas-kmp-default-07.702.10.00-11.sles12sp3.x86_64.compsig; lsi-megaraid_sas-kmp-default-07.702.10.00-11.sles12sp3.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterpriseサーバー 12 (64-bit)カーネルは、次のとおりです。
4.4.21-69-default - SUSE LINUX Enterpriseサーバー12 (64-bit) SP2 plus future errata。
4.4.73-5.1 - SUSE LINUX Enterpriseサーバー12 (64-bit) SP3 plus future errata。

HPE Dynamic Smartアレイ B140i SATA RAID Controller Driver for SUSE LINUX Enterprise Server 12 (64-bit)

バージョン: 1.2.10-139 (A) **(推奨)**
ファイル名: hpdsa-kmp-default-1.2.10-139.sles12sp2.x86_64.rpm; hpdsa-kmp-default-1.2.10-139.sles12sp3.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE Linux Enterprise Server 12(AMD64/EM64T)カーネルは、次の通りです。
3.12.28-4 - SUSE LINUX Enterprise Server 12 (AMD64/EM64T)および将来のアップデートカーネル。
3.12.49-11.1 - SUSE LINUX Enterprise Server 12 (AMD64/EM64T)SP1とさらに将来のerrata。
4.4.21-69-default - SUSE LINUX Enterprise Server 12 (AMD64/EM64T) SP2とさらに将来のerrata

---

HPE Dynamic SmartアレイB140iコントローラードライバーfor VMware vSphere 6.5(ドライバーコンポーネント)

バージョン: 2017.09.25 **(推奨)**
ファイル名: cp032630.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

修正

ドライバーがvmkernel.logに過剰なエラーメッセージを作成する可能性がある1TBを超える物理メモリの問題を修正しました。

HPE Dynamic Smartアレイコントローラードライバー for VMware vSphere 6.5 (バンドルファイル)

バージョン: 5.5.0.60-1 **(推奨)**
ファイル名: hpdsa-5.5.0.60.zip

修正

ドライバーがvmkernel.logに過剰なエラーメッセージを作成する可能性がある1TBを超える物理メモリの問題を修正しました。

HPE H2xx SAS/SATAホストバスアダプタードライバーfor 64-bit Microsoft Windows Server 2016 Edition

バージョン: 2.68.64.2 (B) **(オプション)**

ファイル名: cp032270.exe

重要な注意！

このドライバーコンポーネントは、H221コントローラー搭載のGen9サーバーのみをサポートし、コントローラーはGen9サーバーでのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしません。

拡張

バージョン2.68.64.2(B)に実施された変更:

- Service Pack for ProLiantをバージョン2017.07.0.へ
  注:システムが以前にコンポーネントバージョン2.68.64.2(A)をインストールされている場合、 2.68.64.2(B)にアップデートする必要はありません。

バージョン2.68.64.2(A)の機能改善/新しい機能:

以下のサポートを追加しました。

- Microsoft Windows Server 2016 - Server Core および Server with a Desktop.
- コンポーネントパッケージを改訂しました。この変更によるドライバー機能への変更はありません。システムが以前にドライバーバージョン2.68.64.2にアップデートされている場合、2.68.64.2(A) にアップデートする必要はありません。

サポートしているデバイスおよび機能

このドライバーコンポーネントは、H221コントローラー搭載のGen9サーバーのみをサポートし、コントローラーはGen9サーバーでのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしません

HPE H2xx SAS/SATAホストバスアダプタードライバーfor Microsoft Windows Server 2012 64-ビット Edition

バージョン: 2.68.64.0 (B) **(推奨)**
ファイル名: cp032610.exe

拡張

バージョン2.68.64.0(B)で実装された変更:

- Service Pack for ProLiantをバージョン2017.07.0.へ
  注:ドライバーバージョン2.68.64.0が以前にインストールされている場合は、2.68.64.0(B)にアップデートする必要はありません。

バージョン2.68.64.0の機能改善/新しい機能:

- すべての LSI_sas2 Windowsデバイスのバージョンコントロールを更新

サポートしているデバイスおよび機能

このドライバーコンポーネントは、H221コントローラー搭載のGen9サーバーのみをサポートし、コントローラーはGen9サーバーでのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしません。

HPE H2xx SAS/SATAホストバスアダプタードライバーfor Microsoft Windows Server 2012 R2 64-bit Editions

バージョン: 2.68.64.1 (B) **(オプション)**
ファイル名: cp032453.exe

拡張

バージョン 2.68.64.1(B)に実施された変更:

- Service Pack for ProLiantをバージョン2017.07.0.へ
  注:システムが以前にドライバーバージョン2.68.64.1 にアップデートされている場合、2.68.64.1(B)にアップデートする必要はありません。

バージョン2.68.64.1の機能改善/新しい機能:

- Windows 8.1およびWindows Server 2012R2へのサポートをビルドスクリプトに追加しました。
- Add build support for new 新しいWindowsイベントロギングにビルドサポートを追加しました。
- ビルドの間のデフォルトドライバー・ビルドパラメーターの自動選択にサポートを追加しました。

サポートしているデバイスおよび機能

このドライバーコンポーネントは、H221コントローラー搭載のGen9サーバーのみをサポートし、コントローラーはGen9サーバーでのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしません。

HPE ProLiant Gen10 Smartアレイコントローラードライバーfor VMware ESXi 6.0 (バンドルファイル)

バージョン: 1.0.2.1038-1 **(推奨)**
ファイル名: VMW-ESX-6.0.0-smartpqi-1.0.2.1038-8894171.zip

修正

- VMware vSphere 6.0、6.5、または6.7が動作し、サポートされているディスクエンクロージャへ複数のパスで構成されているシステムでは、単一パスで障害が発生するとディスクへの接続が失われる可能性があります。

HPE ProLiant Gen10 Smartアレイコントローラードライバーfor VMware ESXi 6.5 (バンドルファイル)

バージョン: 1.0.2.1038-1 **(推奨)**
ファイル名: VMW-ESX-6.5.0-smartpqi-1.0.2.1038-8899067.zip

修正

- VMware vSphere 6.0、6.5、または6.7が動作し、サポートされているディスクエンクロージャへ複数のパスで構成されているシステムでは、単一パスで障害が発生するとディスクへの接続が失われる可能性があります。

HPE ProLiant Gen10 Smartアレイコントローラードライバーfor VMware vSphere 6.0 (ドライバーコンポーネント)

バージョン: 2018.07.18 **(推奨)**
ファイル名: cp036830.compsig; cp036830.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

修正

- VMware vSphere 6.0、6.5、または6.7が動作し、サポートされているディスクエンクロージャへ複数のパスで構成されているシステムでは、単一パスで障害が発生するとディスクへの接続が失われる可能性があります。

HPE ProLiant Gen10 Smartアレイコントローラードライバーfor VMware vSphere 6.5 (ドライバーコンポーネント)

バージョン: 2018.07.18 **(推奨)**
ファイル名: cp036831.compsig; cp036831.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

修正

- VMware vSphere 6.0、6.5、または6.7が動作し、サポートされているディスクエンクロージャへ複数のパスで構成されているシステムでは、単一パスで障害が発生するとディスクへの接続が失われる可能性があります。

HPE ProLiant Smartアレイ HPCISSS3コントローラードライバー for 64ビットMicrosoft Windows Server 2012/2012 R2/2016 Editions

バージョン: 100.20.0.64 (A) **(推奨)**
ファイル名: cp033990.exe

拡張

Microsoft Windows 10のサポートを追加しました。

HPE ProLiant Smartアレイコントローラードライバー for VMware vSphere 6.5 (バンドルファイル)

バージョン: 2.0.30-1 **(推奨)**
ファイル名: VMW-ESX-6.5.0-nhpsa-2.0.30-7870290.zip

拡張

- VMware VSANモードを有効にするためにモジュールパラメータを追加しました

HPE ProLiant Smartアレイコントローラードライバー for VMware vSphere 6.5(ドライバーコンポーネント)

バージョン: 2018.06.04 **(推奨)**
ファイル名: cp034542.compsig; cp034542.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

拡張

- VMware VSANモードを有効にするためにモジュールパラメータを追加しました

HPE ProLiant Smartアレイコントローラードライバーfor VMware vSphere 6.0 (ドライバーコンポーネント)

バージョン: 2018.02.12 **(推奨)**
ファイル名: cp033361.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 vmware.comおよびHPE http://vibsdepot.hpe.com/ Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

拡張

PSODイベントの可能性を減らすために、遅いI/O要求完了のドライバー処理を改善しました。

HPE ProLiant Smartアレイコントローラードライバーfor VMware vSphere 6.0 (バンドルファイル)

バージョン: 6.0.0.132-1 **(推奨)**
ファイル名: hpsa-6.0.0.132-7216129.zip

拡張

PSODイベントの可能性を減らすために、遅いI/O要求完了のドライバー処理を改善しました。

HPE SmartアレイGen10コントローラードライバーfor Windows Server 2012 R2およびWindows Server 2016

バージョン: 100.62.0.64 **(推奨)**
ファイル名: cp034601.compsig; cp034601.exe

修正

- Windows 2016はクラスタ検証テストに失敗します。
- Windowsの"削除ポリシー"が誤ってTRUEに設定されています。

HPE SmartアレイS100i SR Gen10 SW RAIDドライバーfor SUSE LINUX Enterprise Server12

バージョン: 1.1.2-155 **(推奨)**
ファイル名: 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

修正

Cannon LakeシステムのID修正。

Red Hat Enterprise Linux (64-bit)用HPE H2xx SAS/SATAバスアダプタードライバー

バージョン: 15.10.08.00-2 **(推奨)**
ファイル名: kmod-mpt2sas-15.10.08.00-1.rhel6u9.x86_64.rpm; kmod-mpt2sas-15.10.08.00-2.rhel6u10.x86_64.rpm

拡張

Red Hat Enterprise Linux 6 Update 10のサポートを追加しました。

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるRed Hat Enterprise Linux 6 (64-bit)カーネルは、次の通りです。
2.6.32-696.el6 - Red Hat Enterprise Linux 6 Update 9(64-bit)およびfuture errata kernels for update 9。
2.6.32-754 - Red Hat Enterprise Linux 6 Update 10(64-bit)および将来のerrata kernels for update 10。

注記:HPE H221ホストバスアダプターは、Gen9サーバーのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしていません。

Red Hat Enterprise Linux (64-bit)用HPE ProLiant Gen10 Smartアレイコントローラー(64-bit)ドライバー

バージョン: 1.1.4-133 (A) **(推奨)**
ファイル名: kmod-smartpqi-1.1.4-133.rhel6u10.x86_64.compsig; kmod-smartpqi-1.1.4-133.rhel6u10.x86_64.rpm; kmod-smartpqi-1.1.4-133.rhel6u9.x86_64.compsig; kmod-smartpqi-1.1.4-133.rhel6u9.x86_64.rpm

修正

Linux Spectreバリアント2脆弱性の問題を解決します

Red Hat Enterprise Linux 6(64-bit)用HPE Dynamic SmartアレイB140i SATA RAIDコントローラードライバー

バージョン: 1.2.10-139 (A) **(推奨)**
ファイル名: kmod-hpdsa-1.2.10-139.rhel6u10.x86_64.rpm; kmod-hpdsa-1.2.10-139.rhel6u9.x86_64.rpm

拡張

Red Hat Enterprise Linux 6 Update 10のサポートを追加しました。

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるRed Hat Enterprise Linux 6 (64-bit)カーネルは、次の通りです。
2.6.32-642.el6 - Red Hat Enterprise Linux 6 Update 8(64-bit)およびfuture errata kernels for update 8。
2.6.32-696.el6 - Red Hat Enterprise Linux 6 Update 9(64-bit)およびfuture errata kernels for update 9。

Red Hat Enterprise Linux 6(64-bit)用HPE ProLiant Smartアレイコントローラー(64-bit)ドライバー

バージョン: 3.4.20-141 (A) **(推奨)**
ファイル名: kmod-hpsa-3.4.20-141.rhel6u10.x86_64.rpm; kmod-hpsa-3.4.20-141.rhel6u9.x86_64.rpm

拡張

Red Hat Enterprise Linux 6 Update 10のサポートを追加しました。

サポートしているデバイスおよび機能

サポートされるカーネル:
このドライバーディスケットでサポートされるRed Hat Enterprise Linux 6 (64-bit)カーネルは、次の通りです。
2.6.32-642.el6 - Red Hat Enterprise Linux 6 Update 8(64-bit)およびfuture errata kernels for update 8。
2.6.32-696.el6 - Red Hat Enterprise Linux 6 Update 9(64-bit)およびfuture errata kernels for update 9。

Red Hat Enterprise Linux 7(64-bit)用HPE Dynamic SmartアレイB140i SATA RAIDコントローラードライバー

バージョン: 1.2.10-139 (A) **(推奨)**

ファイル名: kmod-hpdsa-1.2.10-139.rhel7u4.x86_64.rpm; kmod-hpdsa-1.2.10-139.rhel7u5.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるRed Hat Enterprise Linux 7 (64-bit)カーネルは、次の通りです。
3.10.0-514.el7- Red Hat Enterprise Linux 7 Update 3(64-bit)および future errata kernels for update 3。
3.10.0-693.el7- Red Hat Enterprise Linux 7 Update 4 (64-bit)およびfuture errata kernels for update 4。

Red Hat Enterprise Linux 7(64-bit)用HPE H2xx SAS/SATAバスアダプタードライバー

バージョン: 15.10.08.00-1 **(推奨)**
ファイル名: kmod-mpt2sas-15.10.08.00-1.rhel7u4.x86_64.rpm; kmod-mpt2sas-15.10.08.00-1.rhel7u5.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるRed Hat Enterprise Linux 7 (64-bit)カーネルは、次の通りです。

3.10.0-693.el7- Red Hat Enterprise Linux 7 Update 4 (64-bit)およびfuture errata kernels for update 4.
3.10.0-862.el7- Red Hat Enterprise Linux 7 Update 5 (64-bit)およびUpdate 5用の今後のerrataカーネル。

注記:このドライバーコンポーネントは、H221コントローラー搭載のGen9サーバーのみをサポートし、コントローラーはGen9サーバーでのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしません。

Red Hat Enterprise Linux 7（64-bit）用HPE ProLiant Gen10 Smartアレイ（64-bit）ドライバー

バージョン: 1.1.4-133 (A) **(推奨)**
ファイル名: kmod-smartpqi-1.1.4-133.rhel7u4.x86_64.compsig;kmod-smartpqi-1.1.4-133.rhel7u4.x86_64.rpm; kmod-smartpqi-1.1.4-133.rhel7u5.x86_64.compsig;kmod-smartpqi-1.1.4-133.rhel7u5.x86_64.rpm

修正

Linux Spectreバリアント2脆弱性の問題を解決します

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるRed Hat Enterprise Linux 7 (64-bit)カーネルは、次の通りです。
3.10.0-693.el7- Red Hat Enterprise Linux 7 Update 4 (64-bit)およびUpdate 4用の今後のerrataカーネル。
3.10.0-862.el7- Red Hat Enterprise Linux 7 Update 5 (64-bit)およびUpdate 5用の今後のerrataカーネル。

Red Hat Enterprise Linux 7(64-bit)用HPE ProLiant Smartアレイコントローラー(64-bit)ドライバー

バージョン: 3.4.20-141 (A) **(推奨)**
ファイル名: kmod-hpsa-3.4.20-141.rhel7u4.x86_64.rpm; kmod-hpsa-3.4.20-141.rhel7u5.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるRed Hat Enterprise Linux 7 (64-bit)カーネルは、次の通りです。
3.10.0-514.el7- Red Hat Enterprise Linux 7 Update 3(64-bit)および future errata kernels for update 3。
3.10.0-693.el7- Red Hat Enterprise Linux 7 Update 4 (64-bit)およびfuture errata kernels for update 4。

SUSE LINUX Enterprise Server 11(64-bit)用HPE Dynamic SmartアレイB140i SATA RAIDコントローラードライバー

バージョン: 1.2.10-139 (A) **(推奨)**
ファイル名: hpdsa-kmp-default-1.2.10-139.sles11sp3.x86_64.rpm; hpdsa-kmp-default-1.2.10-139.sles11sp4.x86_64.rpm; hpdsa-kmp-xen-1.2.10-139.sles11sp3.x86_64.rpm; hpdsa-kmp-xen-1.2.10-139.sles11sp4.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリでサポートされるSUSE LINUX Enterpriseサーバー 11 (64-bit)カーネルは、次の通りです。
3.0.76-0.11.1 - SUSE LINUX Enterpriseサーバー11 SP 3 (64-bit)およびfuture errata kernels for SP 3。
3.0.101-63-default - SUSE LINUX Enterpriseサーバー11 SP 4 (64-bit)およびfuture errata kernels for SP 4。

SUSE LINUX Enterprise Server 11(64-bit)用HPE ProLiant Gen10 Smarアレイコントローラー(64-bit)ドライバー

バージョン: 1.1.4-133 (A) **(推奨)**
ファイル名: smartpqi-kmp-default-1.1.4-133.sles11sp4.x86_64.compsig;smartpqi-kmp-default-1.1.4-133.sles11sp4.x86_64.rpm; smartpqi-kmp-xen-1.1.4-133.sles11sp4.x86_64.compsig;smartpqi-kmp-xen-1.1.4-133.sles11sp4.x86_64.rpm

修正

Linux Spectreバリアント2脆弱性の問題を解決します

サポートしているデバイスおよび機能

このドライバーディスケットでサポートされるSUSE LINUX Enterpriseサーバー 11 (64-bit)カーネルは、次の通りです。
3.0.101-63-default - SUSE LINUX Enterpriseサーバー11 SP 4 (64-bit)およびSP4用の今後のerrataカーネル。

SUSE LINUX Enterprise Server 11(64-bit)用HPE ProLiant Smartアレイコントローラー(64-bit)ドライバー

バージョン: 3.4.20-141 (A) **(推奨)**
ファイル名: hpsa-kmp-default-3.4.20-141.sles11sp3.x86_64.rpm; hpsa-kmp-default-3.4.20-141.sles11sp4.x86_64.rpm; hpsa-kmp-xen-3.4.20-141.sles11sp3.x86_64.rpm; hpsa-kmp-xen-3.4.20-141.sles11sp4.x86_64.rpm

サポートしているデバイスおよび機能

このドライバーディスケットでサポートされるSUSE LINUX Enterpriseサーバー 11 (64-bit)カーネルは、次の通りです。
3.0.76-0.11.1 - SUSE LINUX Enterpriseサーバー11 SP 3 (64-bit)およびfuture errata kernels for SP 3。
3.0.101-63-default - SUSE LINUX Enterpriseサーバー11 SP 4 (64-bit)およびfuture errata kernels for SP 4。

SUSE LINUX Enterprise Server 12(64-bit)用HPE Dynamic SmartアレイB140i SATA RAIDコントローラードライバー

バージョン: 1.2.10-135 **(推奨)**
ファイル名: hpdsa-kmp-default-1.2.10-135.sles12sp2.x86_64.rpm; hpdsa-kmp-default-1.2.10-135.sles12sp3.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterpriseサーバー 12 (64-bit)カーネルは、次の通りです。
4.4.21-69-デフォルト- SUSE LINUX Enterpriseサーバー12 (64-bit) SP2 plus future errata。
4.4.73-5.1 - SUSE LINUX Enterpriseサーバー12 (64-bit) SP3 plus future errata。

SUSE LINUX Enterprise Server 12(64-bit)用HPE ProLiant Gen10 Smartアレイ(64-bit)ドライバー

バージョン: 1.1.4-125 **(推奨)**
ファイル名: 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

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterpriseサーバー 12 (64-bit)カーネルは、次の通りです。
4.4.21-69-デフォルト- SUSE LINUX Enterpriseサーバー12 (64-bit) SP2 plus future errata。
4.4.73-5.1 - SUSE LINUX Enterpriseサーバー12 (64-bit) SP3 plus future errata。

SUSE LINUX Enterprise Server 12(64-bit)用HPE ProLiant Gen10 Smartアレイ(64-bit)ドライバー

バージョン: 1.1.4-133 **(推奨)**
ファイル名: smartpqi-kmp-default-1.1.4-133.sles12sp2.x86_64.compsig; smartpqi-kmp-default-1.1.4-133.sles12sp2.x86_64.rpm; smartpqi-kmp-default-1.1.4-133.sles12sp3.x86_64.compsig; smartpqi-kmp-default-1.1.4-133.sles12sp3.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterpriseサーバー 12 (64-bit)カーネルは、次の通りです。
4.4.21-69-デフォルト- SUSE LINUX Enterpriseサーバー12 (64-bit) SP2 plus future errata。
4.4.73-5.1 - SUSE LINUX Enterpriseサーバー12 (64-bit) SP3 plus future errata。

SUSE LINUX Enterprise Server 12(64-bit)用HPE ProLiant Smartアレイコントローラー(64-bit)ドライバー

バージョン: 3.4.20-125 **(推奨)**
ファイル名: hpsa-kmp-default-3.4.20-125.sles12sp2.x86_64.rpm; hpsa-kmp-default-3.4.20-125.sles12sp3.x86_64.rpm

修正

カーネルバッファメッセージ "Inquiry failed"の後にシステムパニックになる問題を修正しました。

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterpriseサーバー 12 (64-bit)カーネルは、次の通りです。
4.4.21-69-default - SUSE LINUX Enterpriseサーバー12 (64-bit) SP2 plus future errata。
4.4.73-5.1 - SUSE LINUX Enterpriseサーバー12 (64-bit) SP3 plus future errata。

SUSE LINUX Enterprise Server 12(64-bit)用HPE ProLiant Smartアレイコントローラー(64-bit)ドライバー

バージョン: 3.4.20-141 (A) **(推奨)**
ファイル名: hpsa-kmp-default-3.4.20-141.sles12sp2.x86_64.rpm; hpsa-kmp-default-3.4.20-141.sles12sp3.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterpriseサーバー 12 (64-bit)カーネルは、次の通りです。
4.4.21-69-default - SUSE LINUX Enterpriseサーバー12 (64-bit) SP2 plus future errata。
4.4.73-5.1 - SUSE LINUX Enterpriseサーバー12 (64-bit) SP3 plus future errata。

SUSE LINUX Enterprise Server 15(64-bit)用HPE Dynamic SmartアレイB140i SATA RAIDコントローラードライバー

バージョン: 1.2.10-139 (A) **(推奨)**
ファイル名: hpdsa-kmp-default-1.2.10-139.sles15sp0.x86_64.rpm

拡張

SUSE LINUX Enterprise Server 15 OSのサポートをリリースしました。

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterpriseサーバー 15(64-bit)カーネルは、次の通りです。
4.12.14-23 - SUSE LINUX Enterpriseサーバー15 (64-bit) SP3 plus future errata。

SUSE LINUX Enterprise Server 15(64-bit)用HPE ProLiant Smartアレイコントローラー(64-bit)ドライバー

バージョン: 3.4.20-141 (A) **(推奨)**
ファイル名: hpsa-kmp-default-3.4.20-141.sles15sp0.x86_64.rpm

拡張

SUSE LINUX Enterprise Server 15 OSのサポートをリリースしました。

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterpriseサーバー 15(64-bit)カーネルは、次の通りです。
4.12.14-23 - SUSE LINUX Enterpriseサーバー15 (64-bit) SP3 plus future errata。

SUSE LINUX Enterrise Server 12(64-bit)用HPE H2xx SAS/SATAバスアダプタードライバー

バージョン: 15.10.06.00-6 **(推奨)**
ファイル名: 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

拡張

SUSE Linux Enterprise Server 12 SP2およびSP3のサポートを追加しました。

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterpriseサーバー 12 (64-bit)カーネルは、次の通りです。
4.4.21-69-デフォルト- SUSE LINUX Enterpriseサーバー12 (64-bit) SP2 plus future errata。
4.4.73-5.1 -SUSE LINUX Enterpriseサーバー12 (64-bit) SP3 plus future errata。

注:このドライバーコンポーネントは、H221コントローラー搭載のGen9サーバーのみをサポートし、コントローラーはGen9サーバーでのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしません。

SUSE LINUX Enterrise Server 12(64-bit)用HPE H2xx SAS/SATAバスアダプタードライバー

バージョン: 15.10.08.00-1 **(推奨)**
ファイル名: lsi-mpt2sas-kmp-default-15.10.08.00-1.sles12sp2.x86_64.rpm; lsi-mpt2sas-kmp-default-15.10.08.00-1.sles12sp3.x86_64.rpm

サポートしているデバイスおよび機能

サポートされるカーネル:
このバイナリrpmでサポートされるSUSE LINUX Enterpriseサーバー 12 (64-bit)カーネルは、次の通りです。
4.4.21-69-デフォルト- SUSE LINUX Enterpriseサーバー12 (64-bit) SP2 plus future errata。
4.4.73-5.1 -SUSE LINUX Enterpriseサーバー12 (64-bit) SP3 plus future errata。

注:このドライバーコンポーネントは、H221コントローラー搭載のGen9サーバーのみをサポートし、コントローラーはGen9サーバーでのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしません。

VMware vSphere 6.0用HPE Dynamic SmartアレイB140iコントローラードライバー(ドライバーコンポーネント)

バージョン: 2018.09.31 **(推奨)**
ファイル名: cp037339.compsig; cp037339.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

修正

ドライバーがデバッグログで過剰なエラーを報告する可能性がある問題を修正します。

VMware vSphere 6.0用HPE Dynamic Smartアレイコントローラードライバー(バンドルファイル)

バージョン: 5.5.0.66-1 **(推奨)**
ファイル名: hpdsa-5.5.0.66.zip

修正

ドライバーがデバッグログで過剰なエラーを報告する可能性がある問題を修正します。

vSphere 6.0用HPE H2xx SAS/SATAホストバスアダプター(64-bit)ドライバー(ドライバーコンポーネント)

バージョン: 2016.03.21 (A) **(オプション)**
ファイル名: cp031478.compsig; cp031478.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

修正

バージョン2016.03.21(A)に実施された変更:

- コンポーネント展開のためにバージョン管理を変更しました。
- Service Pack for ProLiantをバージョン2017.07.0.へ
  注:システムが以前にコンポーネントバージョン2016.03.21にアップデートされている場合、2016.03.21(A)にアップデートする必要はありません。

バージョン2016.03.21で解決した問題:

- なし

拡張

バージョン2016.03.21(A)に実施された変更:

- Service Pack for ProLiantをバージョン2017.07.0.へ
  注:システムが以前にコンポーネントバージョン2016.03.21にアップデートされている場合、2016.03.21(A)にアップデートする必要はありません。

バージョン2016.03.21の機能改善/新しい機能:

- VMWare ESXi 6.0更新1へのサポートが追加されました

サポートしているデバイスおよび機能

注:HPE H221ホストバスアダプターは、Gen9サーバーのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしていません。

vSphere 6.0用HPE SmartアレイP824i-p MRコントローラー(64ビット)ドライバー

バージョン: 7.702.17.00 **(オプション)**
ファイル名: VMW-ESX-6.0.0-lsi_mr3-7.702.17.00-7200103.zip

修正

HPE SmartアレイPクラスMR Gen10コントローラーの初期ドライバーリリース。

vSphere 6.0用HPE SmartアレイP824i-p MRコントローラー(64ビット)ドライバー(ドライバーコンポーネント)

バージョン: 2018.02.12 **(オプション)**
ファイル名: cp032265.compsig; cp032265.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

修正

HPE SmartアレイPクラスMR Gen10コントローラーの初期ドライバーリリース。

---

vSphere 6.5用HPE H2xx SAS/SATAホストバスアダプター(64-bi)ドライバー

バージョン: 15.10.07.00-1 (A) **(オプション)**
ファイル名: mpt2sas-15.10.07.00-esxi5.5-4778920.zip

修正

バージョン15.10.07.00-1(A)実施された変更:

- Service Pack for ProLiantをバージョン2017.07.0.へ
  注:システムが以前にドライバーバージョン15.10.07.00-1にアップデートされている場合、15.10.07.00-1(A)にアップデートする必要はありません。

バージョン15.10.07.00-1で解決した問題:

- VMware vSphere 6.5.ののドライブのインストールに関するマイナートラブルを修正しました。

サポートしているデバイスおよび機能

注:HPE H221ホストバスアダプターは、Gen9サーバーのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしていません。

---

vSphere 6.5用HPE H2xx SAS/SATAホストバスアダプター(64-bi)ドライバー(ドライバーコンポーネント)

バージョン: 2017.01.20 (A) **(オプション)**
ファイル名: cp032277.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

修正

バージョン2017.01.20(A)実施された変更:

- Service Pack for ProLiantをバージョン2017.07.0.へ
  注:システムが以前にコンポーネントバージョン2017.01.20にアップデートされている場合、2017.01.20(A)にアップデートする必要はありません。

バージョン2017.01.20で解決した問題:

- VMware vSphere 6.5.ののドライブのインストールに関するマイナートラブルを修正しました。

サポートしているデバイスおよび機能

注:HPE H221ホストバスアダプターは、Gen9サーバーのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしていません。

---

vSphere 6.5用HPE SmartアレイP824i-p MRコントローラー(64ビット)ドライバー

バージョン: 7.702.17.00 **(オプション)**
ファイル名: VMW-ESX-6.5.0-lsi_mr3-7.702.17.00-7200233.zip

修正

HPE SmartアレイPクラスMR Gen10コントローラーの初期ドライバーリリース。

---

vSphere 6.5用HPE SmartアレイP824i-p MRコントローラー(64ビット)ドライバー(ドライバーコンポーネント)

バージョン: 2018.02.12 **(オプション)**
ファイル名: cp032266.compsig; cp032266.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

修正

HPE SmartアレイPクラスMR Gen10コントローラーの初期ドライバーリリース。

Windows 2012 R2 エディション用HPE Smartアレイ P824i-p MR 64-bitコントローラードライバー

バージョン: 6.714.8.0 **(推奨)**
ファイル名: cp032292.compsig; cp032292.exe

修正

HPE SmartアレイP Class MR Gen10コントローラーの初期ドライバーリリースです。

Windows 2016エディション用HPE Smartアレイ P824i-p MR 64-bitコントローラードライバー

バージョン: 6.714.8.0 **(推奨)**
ファイル名: cp032262.compsig; cp032262.exe

修正

HPE SmartアレイP Class MR Gen10コントローラーの初期ドライバーリリースです。

ドライバー - ストレージファイバーチャネルおよびチャイバーチャネルオーバーイーサーネット

先頭

HPE Storage Fibre Channel Adapter Kit for the x64 Emulex Storport Driver for Windows 2012, Windows 2012R2 and Windows 2016

バージョン: 11.4.334.7 **(推奨)**
ファイル名: cp034221.compsig; cp034221.exe

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class

LPe16000 (16Gb) (FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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

バージョン: 9.2.8.20 **(推奨)**
ファイル名: cp034232.compsig; cp034232.exe

重要な注意！

リリースノート:
HPE StoreFabric QLogic アダプターリリースノート

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

修正

このドライバーバージョンでは、以下が解決しました。

拡張

ドライバーをバージョン9.2.5.21に更新しました

サポートしているデバイスおよび機能

このドライバーは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

HPE Storage Fibre Channel Adapter Kit for the x64 QLogic Storport Driver for Windows Server 2016

バージョン: 9.2.8.20 **(推奨)**
ファイル名: cp034233.compsig; cp034233.exe

重要な注意！

リリースノート:
HPE StoreFabric QLogic アダプターリリースノート

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

修正

このドライバーバージョンでは、以下が解決しました。

拡張

ドライバーバージョン 9.2.5.21

サポートしているデバイスおよび機能

このドライバーは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single PortファイバーチャネルホストバスアダプターHPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual PortファイバーチャネルホストバスアダプターHPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

HPE Storage Fibre Channel Over Ethernet Adapter Kit for the x64 Emulex Storport Driver for Windows 2012, Windows 201R2 and Windows 2016

バージョン: 12.0.1109.0 **(推奨)**
ファイル名: cp034220.compsig; cp034220.exe

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

ドライバーバージョン12.0.1109.0にアップデートしました

rawドライバーファイルフォルダーを削除しました。 rawドライバーファイルは、Smartコンポーネントを解凍し、その後Emulexインストーラーを解凍することによって取得することができます。 次のコマンドを使用します。

brcmdrvr-fcoe-version.exe /q2 extract=2

抽出されたファイルは次に置かれます。

C:¥Users¥Administrator¥Documents¥Broadcom¥Drivers¥FCoE-version

各キットのフォルダーは、それに続くアーキテクチャーとOSフォルダーを持ちます。 例、

C:¥Users¥Administrator¥Documents¥Broadcom¥Drivers¥FCoE-version¥x64¥win2012

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HPE StoreFabric CN1200E-Tアダプター

Red Hat Enterprise Linux 6 Server (x86-64) FC Driver Kit for HPE Qlogic and mezzanine Host Bus Adapters

バージョン: 8.08.00.08.06.0-k1 **(推奨)**
ファイル名: kmod-qlgc-qla2xxx-8.08.00.08.06.0_k1-1.rhel6u8.x86_64.compsig; kmod-qlgc-qla2xxx-8.08.00.08.06.0_k1-1.rhel6u8.x86_64.rpm; kmod-qlgc-qla2xxx-8.08.00.08.06.0_k1-1.rhel6u9.x86_64.compsig; kmod-qlgc-qla2xxx-8.08.00.08.06.0_k1-1.rhel6u9.x86_64.rpm

重要な注意！

リリースノート

HPE StoreFabric QLogic アダプターリリースノート

注記:QLogicドライバーのベース名は、「qlgc」に変更されています。「hpqlgc」ドライバーからのアップデートがサポートされています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

Updated to version 8.07.00.50.06.0-k6

サポートしているデバイスおよび機能

このドライバーは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

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)

バージョン: 12.0.1110.20 **(推奨)**
ファイル名: kmod-brcmfcoe-12.0.1110.20-1.rhel6u8.x86_64.compsig; kmod-brcmfcoe-12.0.1110.20-1.rhel6u8.x86_64.rpm; kmod-brcmfcoe-12.0.1110.20-1.rhel6u9.x86_64.compsig; kmod-brcmfcoe-12.0.1110.20-1.rhel6u9.x86_64.rpm

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

最新のErrata カーネルを使用して、Red Hat Enterprise Linux 6アップデート8(RHEL 6u8)およびRedhat Enterprise Linux 6アップデート9(RHEL 6u9)オペレーティングシステムをアップデートしてください。

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

Updated to Driver version 11.4.1231.0

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE StoreFabric CN1200E-Tアダプター

Red Hat Enterprise Linux 6 Server (x86-64) Fibre Channel Driver Kit for HPE Emulex Host Bus Adapters and mezzanine Host Bus Adapters

バージョン: 11.4.334.26 **(推奨)**
ファイル名: kmod-elx-lpfc-11.4.334.26-1.rhel6u8.x86_64.compsig; kmod-elx-lpfc-11.4.334.26-1.rhel6u8.x86_64.rpm; kmod-elx-lpfc-11.4.334.26-1.rhel6u9.x86_64.compsig; kmod-elx-lpfc-11.4.334.26-1.rhel6u9.x86_64.rpm

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

Driver version 11.4.142.26

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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

バージョン: 8.08.00.08.07.5-k1 **(推奨)**
ファイル名: kmod-qlgc-qla2xxx-8.08.00.08.07.0_k1-1.rhel7u4.x86_64.compsig; kmod-qlgc-qla2xxx-8.08.00.08.07.0_k1-1.rhel7u4.x86_64.rpm; kmod-qlgc-qla2xxx-8.08.00.08.07.5_k1-1.rhel7u5.x86_64.compsig; kmod-qlgc-qla2xxx-8.08.00.08.07.5_k1-1.rhel7u5.x86_64.rpm

重要な注意！

リリースノート:

HPE StoreFabric QLogic アダプターリリースノート

注: QLogicドライバーのベース名は、"qlgc"に変更されています。"hpqlgc" ドライバーからのアップデートがサポートされています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

Updated driver to version 8.07.00.50.07.0-k6

サポートしているデバイスおよび機能

このドライバーは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター

- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

Red Hat Enterprise Linux 7 Server FCoE Driver Kit for HPE Emulex(BRCM) Converged Network Adapters(CNAs) and mezzanine Converged Network Adapters(CNAs)

バージョン: 12.0.1110.20 **(推奨)**
ファイル名: kmod-brcmfcoe-12.0.1110.20-1.rhel7u4.x86_64.compsig; kmod-brcmfcoe-12.0.1110.20-1.rhel7u4.x86_64.rpm; kmod-brcmfcoe-12.0.1110.20-1.rhel7u5.x86_64.compsig; kmod-brcmfcoe-12.0.1110.20-1.rhel7u5.x86_64.rpm

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

最新のErrataカーネルを使用して、Red Hat Enterprise Linux 7アップデート4(RHEL 7u4)オペレーティングシステムをアップデートしてください

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

Updated to Driver version 11.4.1231.0

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE StoreFabric CN1200E-Tアダプター

Red Hat Enterprise Linux 7 Server Fibre Channel Driver Kit for HPE Emulex Host Bus Adapters and mezzanine Host Bus Adapters

バージョン: 11.4.334.26 **(推奨)**
ファイル名: kmod-elx-lpfc-11.4.334.26-1.rhel7u4.x86_64.compsig; kmod-elx-lpfc-11.4.334.26-1.rhel7u4.x86_64.rpm; kmod-elx-lpfc-11.4.334.26-1.rhel7u5.x86_64.compsig; kmod-elx-lpfc-11.4.334.26-1.rhel7u5.x86_64.rpm

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

Driver version 11.4.142.26

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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

バージョン: 8.08.00.08.11.3-k **(推奨)**
ファイル名: qlgc-qla2xxx-kmp-default-8.08.00.08.11.3_k_3.0.101_63-1.sles11sp4.x86_64.compsig; qlgc-qla2xxx-kmp-default-8.08.00.08.11.3_k_3.0.101_63-1.sles11sp4.x86_64.rpm; qlgc-qla2xxx-kmp-default-8.08.00.08.11.3_k_3.0.76_0.11-1.sles11sp3.x86_64.compsig; qlgc-qla2xxx-kmp-default-8.08.00.08.11.3_k_3.0.76_0.11-1.sles11sp3.x86_64.rpm; qlgc-qla2xxx-kmp-xen-8.08.00.08.11.3_k_3.0.101_63-1.sles11sp4.x86_64.compsig; qlgc-qla2xxx-kmp-xen-8.08.00.08.11.3_k_3.0.101_63-1.sles11sp4.x86_64.rpm; qlgc-qla2xxx-kmp-xen-8.08.00.08.11.3_k_3.0.76_0.11-1.sles11sp3.x86_64.compsig; qlgc-qla2xxx-kmp-xen-8.08.00.08.11.3_k_3.0.76_0.11-1.sles11sp3.x86_64.rpm

重要な注意！

リリースノート

HPE StoreFabric QLogic アダプターリリースノート

注: QLogicドライバーのベース名は、"qlgc"に変更されています。"hpqlgc" ドライバーからのアップデートがサポートされています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

Updated driver version 8.07.00.50.11.3-k5

サポートしているデバイスおよび機能

このドライバーは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single PortファイバーチャネルホストバスアダプターHPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual PortファイバーチャネルホストバスアダプターHPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

SUSE Linux Enterprise Server 11 (AMD64/EM64T) FCoE Driver Kit for HPE Emulex(BRCM) Converged Network Adapters(CNAs) and mezzanine Converged Network Adapters(CNAs)

バージョン: 12.0.1110.20 **(推奨)**

ファイル名: brcmfcoe-kmp-default-12.0.1110.20_3.0.101_63-1.sles11sp4.x86_64.compsig; brcmfcoe-kmp-default-12.0.1110.20_3.0.101_63-1.sles11sp4.x86_64.rpm; brcmfcoe-kmp-default-12.0.1110.20_3.0.76_0.11-1.sles11sp3.x86_64.compsig; brcmfcoe-kmp-default-12.0.1110.20_3.0.76_0.11-1.sles11sp3.x86_64.rpm; brcmfcoe-kmp-trace-12.0.1110.20_3.0.101_63-1.sles11sp4.x86_64.compsig; brcmfcoe-kmp-trace-12.0.1110.20_3.0.101_63-1.sles11sp4.x86_64.rpm; brcmfcoe-kmp-trace-12.0.1110.20_3.0.76_0.11-1.sles11sp3.x86_64.compsig; brcmfcoe-kmp-trace-12.0.1110.20_3.0.76_0.11-1.sles11sp3.x86_64.rpm; brcmfcoe-kmp-xen-12.0.1110.20_3.0.101_63-1.sles11sp4.x86_64.compsig; brcmfcoe-kmp-xen-12.0.1110.20_3.0.101_63-1.sles11sp4.x86_64.rpm; brcmfcoe-kmp-xen-12.0.1110.20_3.0.76_0.11-1.sles11sp3.x86_64.compsig; brcmfcoe-kmp-xen-12.0.1110.20_3.0.76_0.11-1.sles11sp3.x86_64.rpm

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

最新のErrataカーネルを持つSuSE Linux Enterprise Server 11 service pack 3(SLES 11sp3)およびSuSE Linux Enterprise Server 11 service pack 4(SLES 11sp4)オペレーティングシステムを更新してください。

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

Updated to Driver version 11.4.1231.0

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE StoreFabric CN1200E-Tアダプター

SUSE Linux Enterprise Server 11 (AMD64/EM64T) Fibre Channel Driver Kit for HPE Emulex Host Bus Adapters and mezzanine Host Bus Adapters

バージョン: 11.4.334.26 **(推奨)**
ファイル名: elx-lpfc-kmp-default-11.4.334.26_3.0.101_63-1.sles11sp4.x86_64.compsig; elx-lpfc-kmp-default-11.4.334.26_3.0.101_63-1.sles11sp4.x86_64.rpm; elx-lpfc-kmp-default-11.4.334.26_3.0.76_0.11-1.sles11sp3.x86_64.compsig; elx-lpfc-kmp-default-11.4.334.26_3.0.76_0.11-1.sles11sp3.x86_64.rpm; elx-lpfc-kmp-trace-11.4.334.26_3.0.101_63-1.sles11sp4.x86_64.compsig; elx-lpfc-kmp-trace-11.4.334.26_3.0.101_63-1.sles11sp4.x86_64.rpm; elx-lpfc-kmp-trace-11.4.334.26_3.0.76_0.11-1.sles11sp3.x86_64.compsig; elx-lpfc-kmp-trace-11.4.334.26_3.0.76_0.11-1.sles11sp3.x86_64.rpm; elx-lpfc-kmp-xen-11.4.334.26_3.0.101_63-1.sles11sp4.x86_64.compsig; elx-lpfc-kmp-xen-11.4.334.26_3.0.101_63-1.sles11sp4.x86_64.rpm; elx-lpfc-kmp-xen-11.4.334.26_3.0.76_0.11-1.sles11sp3.x86_64.compsig; elx-lpfc-kmp-xen-11.4.334.26_3.0.76_0.11-1.sles11sp3.x86_64.rpm

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

最新のErrataカーネルを持つSuSE Linux Enterprise Server 11 service pack 3(SLES 11sp3)およびSuSE Linux Enterprise Server 11 service pack 4(SLES 11sp4)オペレーティングシステムを更新してください。

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

Driver version 11.4.142.26

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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

バージョン: 8.08.00.07.12.3-k1 **(推奨)**
ファイル名: 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

重要な注意！

リリースノート:

HPE StoreFabric QLogic アダプターリリースノート

注: QLogicドライバーのベース名は、"qlgc"に変更されています。"hpqlgc" ドライバーからのアップデートがサポートされています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

修正

このドライバーバージョンでは、以下が解決しました。

- ドライバーリトライカウントを30に増加しました。
- ターゲットからのDIFエラーを再試行可能エラーとしてマークします。
- 27xx fwdump中の過剰なデバッグプリントを低減しました。
- exit_creds()のnull credポインターのcrashを回避しました。
- classic fwdumpのmbxポインターエラーを修正しました。
- 異なる種類のRSCNのチェックを追加しました。
- 不正なfcport_countアカウンティングを修正しました。
- sysfsについて、サポートされているFC速度を修正しました。
- FDMI/RDPについて、サポートされているFC速度を修正しました。

拡張

Updated to version 8.07.00.50.12.3-k6

サポートしているデバイスおよび機能

このドライバーは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

SUSE Linux Enterprise Server 12 FC Driver Kit for HPE QLogic and mezzanine Host Bus Adapters

バージョン: 8.08.00.08.12.3-k1 **(推奨)**
ファイル名: qlgc-qla2xxx-kmp-default-8.08.00.08.12.2_k1_k4.4.21_69-1.sles12sp2.x86_64.compsig; qlgc-qla2xxx-kmp-default-8.08.00.08.12.2_k1_k4.4.21_69-1.sles12sp2.x86_64.rpm; qlgc-qla2xxx-kmp-default-8.08.00.08.12.3_k1_k4.4.73_5-1.sles12sp3.x86_64.compsig; qlgc-qla2xxx-kmp-default-8.08.00.08.12.3_k1_k4.4.73_5-1.sles12sp3.x86_64.rpm

重要な注意！

リリースノート:

HPE StoreFabric QLogic アダプターリリースノート

注: QLogicドライバーのベース名は、"qlgc"に変更されています。"hpqlgc" ドライバーからのアップデートがサポートされています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

Updated to version 8.07.00.50.12.3-k6

サポートしているデバイスおよび機能

このドライバーは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single PortファイバーチャネルホストバスアダプターHPE StoreFabric SN1600Q 32Gb Dual PortファイバーチャネルホストバスアダプターHPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

SUSE Linux Enterprise Server 12 FCoE Driver Kit for HPE Emulex(BRCM) Converged Network Adapters(CNAs) and mezzanine Converged Network Adapters(CNAs)

バージョン: 12.0.1110.11 **(推奨)**
ファイル名: 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

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

ドライバーバージョン12.0.1110.11にアップデートしました

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HPE StoreFabric CN1200E-Tアダプター

SUSE Linux Enterprise Server 12 FCoE Driver Kit for HPE Emulex(BRCM) Converged Network Adapters(CNAs) and mezzanine Converged Network Adapters(CNAs)

バージョン: 12.0.1110.20 **(推奨)**

ファイル名: brcmfcoe-kmp-default-12.0.1110.20_k4.4.21_69-1.sles12sp2.x86_64.compsig; brcmfcoe-kmp-default-12.0.1110.20_k4.4.21_69-1.sles12sp2.x86_64.rpm; brcmfcoe-kmp-default-12.0.1110.20_k4.4.73_5-1.sles12sp3.x86_64.compsig; brcmfcoe-kmp-default-12.0.1110.20_k4.4.73_5-1.sles12sp3.x86_64.rpm

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

最新のErrataカーネルを持つSuSE Linux Enterprise Server 12 service pack 2(SLES 12sp2)およびSuSE Linux Enterprise Server 12 service pack 3(SLES 12sp3)オペレーティングシステムを更新してください。

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

Updated to Driver version 11.4.1231.0

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター

- HPE StoreFabric CN1200E-Tアダプター

SUSE Linux Enterprise Server 12 Fibre Channel Driver Kit for HPE Emulex Host Bus Adapters and mezzanine Host Bus Adapters

バージョン: 11.4.334.12 **(推奨)**
ファイル名: 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

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

最新のErrataカーネルを持つSuSE Linux Enterprise Server 12 service pack 3(SLES 12sp3)オペレーティングシステムを更新してください。

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

ドライバーバージョン11.4.334.12にアップデートしました

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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 Fibre Channel Driver Kit for HPE Emulex Host Bus Adapters and mezzanine Host Bus Adapters

バージョン: 11.4.334.26 **(推奨)**
ファイル名: elx-lpfc-kmp-default-11.4.334.26_k4.4.103_6.38-1.sles12sp3.x86_64.compsig; elx-lpfc-kmp-default-11.4.334.26_k4.4.103_6.38-1.sles12sp3.x86_64.rpm; elx-lpfc-kmp-default-11.4.334.26_k4.4.21_69-1.sles12sp2.x86_64.compsig; elx-lpfc-kmp-default-11.4.334.26_k4.4.21_69-1.sles12sp2.x86_64.rpm

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

最新のErrataカーネルを持つSuSE Linux Enterprise Server 12 service pack 2(SLES 12sp2)およびSuSE Linux Enterprise Server 12 service pack 3(SLES 12sp3)オペレーティングシステムを更新してください。

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

Driver version 11.4.142.26

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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

ドライバー - システム

先頭

HP HPE NVDIMM-N ドライバー for Microsoft Windows Server 2012および2012 R2

バージョン: 2.0.0.2 **(推奨)**
ファイル名: cp031329.compsig; cp031329.exe

拡張

これらのNVDIMM-Nドライバーは Microsoft Windows Server 2012および2012 R2をを実行する限定されたHPEサーバー上での永続的メモリに関するサポートを可能にします。

- HPE 16GB NVDIMMデバイスのサポートを追加しました。
- ブロックセクターサイズを512バイトから4096バイトに変更しました。 古いデータを保存する必要がある場合には、アクセスできないようにしてバックアップしなければなりません。

HPEサーバー上の永続的メモリに関する詳しい情報については、下記のリンクを参照願います。

- https://www.hpe.com/us/en/servers/management.html
- http://h20195.www2.hpe.com/V2/GetDocument.aspx?docname=4AA6-4681ENW&cc=us&lc=en

---

ドライバー - システムマネジメント

先頭

HPE ProLiant Gen9チップセット識別子 for Windows Server 2012からServer 2016

バージョン: 10.1.2.77 (B) **(オプション)**
ファイル名: cp035099.exe

修正

Windows Device Guardが有効になっているときに発生する可能性のあるインストール エラーを修正しました。

---

iLO 3/4チャネルインターフェイスドライバーfor Windows Server 2012およびWindows Server 2012 R2

バージョン: 3.31.0.0 **(推奨)**
ファイル名: cp036919.exe

重要な注意！

ProLiant Support Packバージョン9.00がリリースされたときに、チャネルインターフェイスドライバーが独自のコンポーネントに分割されました。 以前、ドライバーは、*iLO 3* マネジメントコントローラードライバーパッケージのコンポーネントの一部でした。

修正

iLOリモートコンソールまたはiLO仮想メディアの使用中に発生する可能性のあるWindowsバグチェック(DPC_WATCHDOG_VIOLATION)を修正しました。

---

iLO 3/4チャネルインターフェースドライバー for Windows Server 2008 および Windows Server 2012 R2

バージョン: 3.30.0.0 **(オプション)**
ファイル名: cp029394.exe

重要な注意！

ProLiant Support Packバージョン9.00がリリースされたときに、チャネルインターフェイスドライバーが独自のコンポーネントに分割されました。 以前、ドライバーは、*iLO 3* マネジメントコントローラードライバーパッケージのコンポーネントの一部でした。

修正

ドライバーを再起動した場合、ドライバーで作成された作業項目が適切に終了していることを確認してください

---

iLO 3/4マネージメントコントローラードライバーパッケージ for Windows Server 2008から2012 R2

バージョン: 3.30.0.0 **(オプション)**
ファイル名: cp029429.exe

事前要件

このコンポーネントの前に*HP ProLiant iLO 3/4 Channel Interface Driver for Windows Server 2008 to Server 2012 R2*(バージョン3.4.0.0以降)をインストールする必要があります。チャネルインターフェイスドライバーは、以前はこのコンポーネントに含まれていましたが、現在は別々にインストールされます。

拡張

ProLiant System Shutdown サービスで提供されたサポートは、ProLiant Monitor サービスへ統合されました。ProLiant System Shutdown サービスは、システムのサービスリスト内で個別項目としては表示されません。

---

iLO 3/4マネジメントコントローラードライバーパッケージ for Windows Server 2016

バージョン: 3.30.0.0 **(オプション)**
ファイル名: cp030672.exe

事前要件

このコンポーネントの前に*HP ProLiant iLO 3/4 Channel Interface Driver for Windows Server 2016*(バージョン3.4.0.0以降)をインストールする必要があります。

拡張

Windows Server 2016をサポートする最初のリリースです。

---

iLO 4 チャネルインターフェースドライバー for Windows Server 2016

バージョン: 3.31.0.0 **(推奨)**
ファイル名: cp034683.exe

修正

iLOリモートコンソールまたはiLO仮想メディアの使用中に発生する可能性のあるWindowsバグチェック(DPC_WATCHDOG_VIOLATION)を修正しました。

---

iLO 5 チャネルインターフェースドライバー for Windows Server 2012 R2

バージョン: 4.3.0.0 **(オプション)**
ファイル名: cp034070.compsig; cp034070.exe

拡張

- iLO 5のユニバーサルシリアルバスコントローラーとの中断共有を避けるためにメッセージシグナル割り込みを有効にしました。
- HPE ProLiant DL325 Gen10のサポートを追加しました。

---

iLO 5 チャネルインターフェースドライバー for Windows Server 2016
バージョン: 4.3.0.0 **(オプション)**
ファイル名: cp034071.compsig; cp034071.exe

拡張

- iLO 5のユニバーサルシリアルバスコントローラーとの中断共有を避けるためにメッセージシグナル割り込みを有効にしました。
- HPE ProLiant DL325 Gen10のサポートを追加しました。

Windows Server 2012 R2用iLO 5自動サーバー復旧ドライバー
バージョン: 4.2.0.0 (B) **(オプション)**
ファイル名: cp034068.compsig; cp034068.exe

重要な注意！

iLO 5 Channel Interface Driver(バージョン4.1.0.0以前)をインストールすると、このドライバーが上書きされます。上書きを避けるには、バージョン4.1.0.0(B)以降のiLO 5 Channel Interface Driverを使用してください。

拡張

HPE ProLiant DL325 Gen10のサポートを追加しました。

Windows Server 2016用iLO 5自動サーバー復旧ドライバー
バージョン: 4.2.0.0 (B) **(オプション)**
ファイル名: cp034069.compsig; cp034069.exe

重要な注意！

iLO 5 Channel Interface Driver(バージョン4.1.0.0以前)をインストールすると、このドライバーが上書きされます。上書きを避けるには、バージョン4.1.0.0(B)以降のiLO 5 Channel Interface Driverを使用してください。

拡張

HPE ProLiant DL325 Gen10のサポートを追加しました。

ドライバー - ビデオ
先頭

Matrox G200eH3ビデオコントローラードライバー for Windows Server 2016
バージョン: 9.15.1.184 (B) **(オプション)**
ファイル名: cp033124.compsig; cp033124.exe

拡張

HPE ProLiant DL325 Gen10のサポートを追加しました。

Matrox G200eHビデオコントローラードライバー for Windows Server 2012および2012 R2
バージョン: 9.15.1.184 **(オプション)**
ファイル名: cp032302.exe

拡張

9.15.1.174リリースと比較してビデオ性能が改善されました。

Matrox G200eHビデオコントローラードライバー for Windows Server 2016

バージョン: 9.15.1.184 **(オプション)**
ファイル名: cp032303.exe

拡張

9.15.1.174リリースと比較してビデオ性能が改善されました。

Windows Server 2012 R2用Matrox G200eH3ビデオコントローラードライバー

バージョン: 9.15.1.184 (B) **(オプション)**
ファイル名: cp033123.compsig; cp033123.exe

拡張

HPE ProLiant DL325 Gen10のサポートを追加しました。

ファームウェア - ブレードインフラストラクチャ

先頭

HPE BladeSystem c-Class Virtual Connectファームウェア、Ethernet plus 8 Gb 20ポートおよび8/16 Gb 24ポートFC Editionコンポーネント for Linux

バージョン: 4.62 **(推奨)**
ファイル名: RPMS/i386/firmware-vceth-4.62-1.1.i386.rpm

事前要件

『HPE Virtual Connectリリースノート』のバージョン4.62には、前提条件が含まれていて、次のURLにあります:http://www.hpe.com/info/vc/manuals

修正

バージョン4.62で解決した問題のリストは、http://www.hpe.com/info/vc/manualsにあるHPE Virtual Connectリリースノートに記載されています。

拡張

バージョン4.62での機能強化のリストは、http://www.hpe.com/info/vc/manualsにあるHPE Virtual Connectリリースノートに記載されています。

サポートしているデバイスおよび機能

HPE Flex-10 10Gb Virtual Connect Ethernetモジュール for c-Class BladeSystem

HPE Virtual Connect FlexFabric 10Gb/24ポートモジュール for c-Class BladeSystem

HPE Virtual Connect 8Gb 24ポート ファイバーチャネルモジュール for c-Class BladeSystem

HPE Virtual Connect 8Gb 20ポート ファイバーチャネルモジュール for c-Class BladeSystem

HPE Virtual Connect Flex-10/10Dモジュール for c-Class BladeSystem

HPE Virtual Connect FlexFabric-20/40 F8モジュール for HP BladeSystem c-Class

HPE Virtual Connect 16Gb 24ポート ファイバーチャネルモジュール for c-Class BladeSystem

HPE BladeSystem c-Class Virtual Connectファームウェア、Ethernet plus 8Gb 20ポートおよび8/16 Gb 24ポートFC Editionコンポーネントfor Windows

バージョン: 4.62 **(推奨)**
ファイル名: cp034382.exe

事前要件

HPE Virtual Connectリリースノートのバージョン4.62には、前提条件が含まれていて、次のURLにあります:http://www.hpe.com/info/vc/manuals

修正

バージョン4.62で解決した問題のリストは、http://www.hpe.com/info/vc/manualsにあるHPE Virtual Connectリリースノートに記載されています。

拡張

バージョン4.62での機能強化のリストは、http://www.hpe.com/info/vc/manualsにあるHPE Virtual Connectリリースノートに記載されています。

サポートしているデバイスおよび機能

HPE Flex-10 10Gb Virtual Connect Ethernetモジュール for c-Class BladeSystem

HPE Virtual Connect FlexFabric 10Gb/24ポートモジュール for c-Class BladeSystem

HPE Virtual Connect 8Gb 24ポート ファイバーチャネルモジュール for c-Class BladeSystem

HPE Virtual Connect 8Gb 20ポート ファイバーチャネルモジュール for c-Class BladeSystem

HPE Virtual Connect Flex-10/10Dモジュール for c-Class BladeSystem

HPE Virtual Connect FlexFabric-20/40 F8モジュール for HP BladeSystem c-Class

HPE Virtual Connect 16Gb 24ポート ファイバーチャネルモジュール for c-Class BladeSystem

---

オンラインHP 6Gb SAS BLスイッチファームウェア Smart Component for Linux (x86/x64)

バージョン: 4.3.6.0 **(オプション)**
ファイル名: RPMS/i586/firmware-solex6gb-solex-4.3.6.0-1.1.i586.rpm

拡張

D6020、D3610、およびD3710のサポートを追加しました

オンラインHPE 6 Gb SAS BLスイッチファームウェアSmart Component for Windows (x86/x64)

バージョン: 4.3.6.0 **(オプション)**
ファイル名: cp034920.exe

拡張

D6020、D3610、およびD3710のサポートを追加しました

オンラインHPE BladeSystem c-Class Onboard Administratorファームウェアコンポーネント for Linux

バージョン: 4.85 **(推奨)**

ファイル名: RPMS/x86_64/firmware-oa-4.85-1.1.x86_64.rpm

重要な注意！

重要な注意

- **ファームウェアアップグレード**
  - Starting OA 4.50のリリースを開始するにあたって、ファームウェアのイメージの信頼性を強化するために標準化されたコード署名と認証のメカニズムが導入されています。
  - ファームウェアのROMイメージを使用している顧客がOAをアップグレードすることに関して
    - ファームウェアバージョンが3.50以前のOAに関して, まずOAを3.50にアップグレードし、それからOA 4.50以降へのアップグレードを続けます。
  - Smart コンポーネントを使用している顧客がOAをアップグレードすることに関して
    - HPE Smart コンポーネントに依存するOAファームウェアのアップグレードメカニズム(例:EFM)は、この変更に影響を受けません。Smartコンポーネントは OA 4.50以降へのアップグレードを行う前に、OA 3.50への中間アップグレードを行います。
- **EFM**
  - OAは4 GB以下のサイズのSPP ISOイメージだけをサポートします。エンクロージャーDVD形式で直接 保存されているか、付随したUSBキーか、特定のURL経由で遠隔でマウントされているかのどれかとなります。もしISOイメージが4 GBを越える場合、CLI SHOW FIRMWARE MANAGEMENTコマンドはISO URLステータスを"Invalid URL"と表示します。
  - SPP ISOイメージが4 GB以上である場合、OA EFMブレードファームウェアの更新プロセスには不要なコンポーネントを除外したカスタムISOイメージを作成する必要があります。 カスタムISOには、少なくともHPE ProLiant BLシリーズのサーバー用ファームウェアコンポーネントだけは含める必要があります。(カスタムISO画像を作成するためにHP SUMを使用しているときは、コンポーネントの種類としてファームウェアを選択し、サーバーの種類としてHPE ProLiant BLシリーズを選択してください。)OA EFM機能に交換性があるカスタムISO画像の作成の情報については、『HPE BladeSystem Onboard Administratorユーザーガイド』をご覧ください。HP SUMに関する詳しい情報はHPE Smart Update Managerのオンラインヘルプまたは次で見つけることができます。https://www.hpe.com/servers/hpsum/documentation
- **FIPS**
  - OA 4.40は、http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdfにある140-2 In Process Listで参照されるようにFIPSのアクティブ評価中です。
- **IPv6**
  - DHCPv6の有効化またはSLAACエンクロージャーIPv6設定の有効化がOnboard Administrator上で無効にされている場合、それらそれぞれの構成に基づいて、これらのアドレスが自動的に期限切れになるまで、エンクロージャー内のiLOのそれぞれのDHCPv6またはSLAACアドレスは保持されます。 iLOのマニュアルリセットはすぐにこれらのアドレスを解放します。

事前要件

Onboard Administrator Smartコンポーネントは、32ビット実行可能バイナリを含みます。 その結果、OA Smartコンポーネントがインストールされ、実行されるクライアントオペレーティングシステムは、32ビット実行可能ファイルのネイティブサポートを持つか、インストールされた32ビット互換ライブラリを持つ必要があります。

修正

全般

- Onboard Administrator のフェイルオーバー後に送信されなかった SNMPトラップ cpqRackEnclosureManagerLinkUpの問題に対処します。
- Onboard Administratorの以前のバージョンに見られたオンラインヘルプのコンテンツの問題を解決します。

セキュリティ

以下のセキュリティの脆弱性が修正されました:

- CVE-2017-8105 - バッファ オーバーフローにより起こるメモリ破損の脆弱性に対処しました。
- CVE-2016-10244 – リモートの攻撃者が細工されたファイルを介してサービス拒否を引き起こす可能性のある脆弱性に対処しました。

問題点および解決策

ブラウザー

- OA GUIはChromeのバージョン43.0.2357.10から44.0.2383ではアクセスできません。この問題は、Chrome(またはWebKit)の"回帰"によって発生しています。FirefoxやInternet Explorerなどの代わりのブラウザーを使用するか、別のバージョンのChromeを試す必要があります。
- iLOホスト名を使用したOAからのSSO-to-iLO接続は、Windows 8のMicrosoft Internet Explorer 11で失敗します。Internet Explorer 10またはInternet Explorer 11を備えたWindows 8システムでは、OA Web GUIセッションがIPアドレスの代わりにホスト名を使用してロードされている場合、OA Web GUIからSSOを使用してiLOウィンドウを開こうとすると、目的の新しいウィンドウではなくOA Web GUIウィンドウにiLOページが読み込まれる可能性があります。この問題はInternet Explorerのバグであると判断され、Internet Explorerの将来のリリースまたはアップデートで修正される予定です。この問題を回避するには、IPアドレスを使用してOA Web GUIをロードするか、Internet Explorerの設定で適切なゾーンの保護モードをオフにします。この問題はInternet Explorerブラウザーのみで発生します。

FIPS

2048ビット未満のサイズの証明書は、OA 4.20以降のOAファームウェアによって強制されるFIPS要件に準拠していません。OAファームウェアバージョン4.40以降を実行しているOAがFIPSモードON/DEBUGで動作し、以前のバージョンのOAファームウェアを実行しているときにインストールされた1024ビットのLDAP証明書で構成されている場合、非準拠の証明書が存在するためにFIPSモードON/DEBUGは劣化状態で動作しているとみなされます。このFIPS-劣化モードで動作している間に、OA GUIのネットワークアクセス>FIPSタブからFIPSモードをオフに設定しようとすると失敗し、選択したFIPSモードが既に有効になっているというエラーメッセージが表示されます。非準拠の証明書が削除されると、FIPS-劣化モードの動作ステータスはクリアされ、FIPSモードはGUIインターフェイスから正常にOFFに設定できます。OA CLIコマンドSET FIPS MODE OFFを使用すると、OAにインストールされている非準拠の1024ビットLDAP証明書を使用しても、FIPSモードをオフに設定できます。

IRC

Gen10 Blade用の.net IRCコンソールを開くことができない、Gen9 Bladeも同じ問題があります。JavaアプレットとWebstartはロードされますが、仮想メディアのマウントは失敗します。回避策として、ターミナルクライアントにインストールされているIRCアプリケーション(HP Lights-Outスタンドアロンリモートコンソール)を使用してIRCを起動することです。

EFM

Gen 10 BladeでEFMを使用するには、HPSUM 8.0.0でカスタムSPP ISOを作成する際にオプション/フィルター"*Make Bootable ISO file*"と"*Enclosure Firmware Management*"を選択してください。詳細については、HPSUM 8.0.0ユーザーガイドを参照してください。

CAC

- CACモードのSSHでは、TelnetおよびXML応答プロトコルは無効になります。
- リンクされたエンクロージャーがCACモードになっている場合、リンクされたエンクロージャーのログインは動作しません。
- サービスアカウントの詳細を正確に指定しないと、証明書を使用したLDAPユーザーのログインは失敗します。
- CACの使用を開始する前にリカバリプランを立てることを強くお勧めします。 OA設定で問題が起こった場合、OAをシリアルポートまたはInsight DisplayパネルおよびUSB KEYからリカバリできる場合があります。いずれの方法もOAへの物理アクセスが必要です。 ただし、LCD PINが設定されている(または忘れた)場合、およびローカルアカウントが無効になっているかCACが正しく設定されていない場合、リカバリする唯一の方法はシリアルポート経由です。OAの復旧が必要な最も一般的な状況を2つ挙げると、LDAPが無効なローカルアカウントで誤って設定されている場合と、CACが証明書にアクセスしないよう設定されている場合です。

設定可能なSSHポート番号

スタンバイOAが4.85未満のファームウェアバージョンを実行していて、アクティブOAのファームウェア同期機能を使用してファームウェアバージョンが4.85以上に更新した場合、ファームウェアのアップデートおよびスタンバイOAの再起動後、SSHポートは構成されたポート番号で開きません。回避策は、スタンバイOAを再起動することです。SSHポートは、次回起動時に設定されたポートで開きます。SSH ポートがアクティブOAのデフォルトポート22で構成されている場合は、この問題が発生しません。

拡張

Onboard Administrator 4.85は、以下の機能強化に対するサポートを提供します:

ハードウェアの追加

- HPE D2500sb Storage Blade

特徴**: 追加と変更**

全般

- Onboard AdministratorがSNMPエンジンIDとして、IPv6 アドレスを構成できるように拡張されました。
- Onboard Administrator が SSH ポート番号を定義するユーザーを構成できるように拡張されました。これにより、ユーザーはデフォルトのSSHポート22ではなく非標準のSSHポートを設定できます。

セキュリティ

一般的なデータ保護要件(GDPR)サポートは、HPE EmbeddedリモートサポートソリューションのOnboard Administratorに追加されています。HPEパスポートのユーザー名は暗号化された形式で保存されます。

オンラインHPE BladeSystem c-Class Onboard Administratorファームウェアコンポーネント for Windows

バージョン: 4.85 **(推奨)**
ファイル名: cp034861.exe

重要な注意！

重要な注意

- **ファームウェアアップグレード**
  - Starting OA 4.50のリリースを開始するにあたって、ファームウェアのイメージの信頼性を強化するために標準化されたコード署名と認証のメカニズムが導入されています。
  - ファームウェアのROMイメージを使用している顧客がOAをアップグレードすることに関して
    - ファームウェアバージョンが3.50以前のOAに関して, まずOAを3.50にアップグレードし、それからOA 4.50以降へのアップグレードを続けます。
  - Smart コンポーネントを使用している顧客がOAをアップグレードすることに関して
    - HPE Smart コンポーネントに依存するOAファームウェアのアップグレードメカニズム(例:EFM)は、この変更に影響を受けません。Smartコンポーネントは OA 4.50以降へのアップグレードを行う前に、OA 3.50への中間アップグレードを行います。
- **EFM**
  - OAは4 GB以下のサイズのSPP ISOイメージだけをサポートします。エンクロージャーDVD形式で直接 保存されているか、付随したUSBキーか、特定のURL経由で遠隔でマウントされているかのどれかとなります。もしISOイメージが4 GBを越える場合、CLI SHOW FIRMWARE MANAGEMENTコマンドはISO URLステータスを"Invalid URL"と表示します。
  - SPP ISOイメージが4 GB以上である場合、OA EFMブレードファームウェアの更新プロセスには不要なコンポーネントを除外したカスタムISOイメージを作成する必要があります。 カスタムISOには、少なくともHPE ProLiant BLシリーズのサーバー用ファームウェアコンポーネントだけは含める必要があります。(カスタムISO画像を作成するためにHP SUMを使用しているときは、コンポーネントの種類としてファームウェアを選択し、サーバーの種類としてHPE ProLiant BLシリーズを選択してください。)OA EFM機能に交換性があるカスタムISO画像の作成の情報については、『HPE BladeSystem Onboard Administrator ユーザーガイド』をご覧ください。HP SUMに関する詳しい情報はHPE Smart Update Managerのオンラインヘルプまたは次で見つけることができます。https://www.hpe.com/servers/hpsum/documentation
- **FIPS**
  - OA 4.40は、http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdfにある140-2 In Process Listで参照されるようにFIPSのアクティブ評価中です。
- **IPv6**
  - DHCPv6の有効化またはSLAACエンクロージャーIPv6設定の有効化がOnboard Administrator上で無効にされている場合、それらそれぞれの構成に基づいて、これらのアドレスが自動的に期限切れになるまで、エンクロージャー内のiLOのそれぞれのDHCPv6またはSLAACアドレスは保持されます。 iLOのマニュアルリセットはすぐにこれらのアドレスを解放します。

事前要件

Onboard Administrator Smartコンポーネントは、32ビット実行可能バイナリを含みます。 その結果、OA Smartコンポーネントがインストールされ、実行されるクライアントオペレーティングシステムは、32ビット実行可能ファイルのネイティブサポートを持つか、インストールされた32ビット互換ライブラリを持つ必要があります。

修正

全般

- Onboard Administrator のフェイルオーバー後に送信されなかった SNMPトラップ cpqRackEnclosureManagerLinkUpの問題に対処します。
- Onboard Administratorの以前のバージョンに見られたオンラインヘルプのコンテンツの問題を解決します。

セキュリティ

以下のセキュリティの脆弱性が修正されました:

- CVE-2017-8105 - バッファ オーバーフローにより起こるメモリ破損の脆弱性に対処しました。
- CVE-2016-10244 – リモートの攻撃者が細工されたファイルを介してサービス拒否を引き起こす可能性のある脆弱性に対処しました。

問題点および解決策

ブラウザー

- OA GUIはChromeのバージョン43.0.2357.10から44.0.2383ではアクセスできません。この問題は、Chrome(またはWebKit)の"回帰"によって発生しています。FirefoxやInternet Explorerなどの代わりのブラウザーを使用するか、別のバージョンのChromeを試す必要があります。
- iLOホスト名を使用したOAからのSSO-to-iLO接続は、Windows 8のMicrosoft Internet Explorer 11で失敗します。Internet Explorer 10またはInternet Explorer 11を備えたWindows 8システムでは、OA Web GUIセッションがIPアドレスの代わりにホスト名を使用してロードされている場合、OA Web GUIからSSOを使用してiLOウィンドウを開こうとすると、目的の新しいウィンドウではなくOA Web GUIウィンドウにiLOページが読み込まれる可能性があります。この問題はInternet Explorerのバグであると判断され、Internet Explorerの将来のリリースまたはアップデートで修正される予定です。この問題を回避するには、IPアドレスを使用してOA Web GUIをロードするか、Internet Explorerの設定で適切なゾーンの保護モードをオフにします。この問題はInternet Explorerブラウザーのみで発生します。

FIPS

2048ビット未満のサイズの証明書は、OA 4.20以降のOAファームウェアによって強制されるFIPS要件に準拠していません。OAファームウェアバージョン4.40以降を実行しているOAがFIPSモードON/DEBUGで動作し、以前のバージョンのOAファームウェアを実行しているときにインストールされた1024ビットのLDAP証明書で構成されている場合、非準拠の証明書が存在するためにFIPSモードON/DEBUGは劣化状態で動作しているとみなされます。このFIPS-劣化モードで動作している間に、OA GUIのネットワークアクセス>FIPSタブからFIPSモードをオフに設定しようとすると失敗し、選択したFIPSモードが既に有効になっているというエラーメッセージが表示されます。非準拠の証明書が削除されると、FIPS-劣化モードの動作ステータスはクリアされ、FIPSモードはGUIインターフェイスから正常にOFFに設定できます。OA CLIコマンドSET FIPS MODE OFFを使用すると、OAにインストールされている非準拠の1024ビットLDAP証明書を使用しても、FIPSモードをオフに設定できます。

IRC

Gen10 Blade用の.net IRCコンソールを開くことができない、Gen9 Bladeも同じ問題があります。JavaアプレットとWebstartはロードされますが、仮想メディアのマウントは失敗します。回避策として、ターミナルクライアントにインストールされているIRCアプリケーション(HP Lights-Outスタンドアロンリモートコンソール)を使用してIRCを起動することです。

EFM

Gen 10 BladeでEFMを使用するには、HPSUM 8.0.0でカスタムSPP ISOを作成する際にオプション/フィルター"*Make Bootable ISO file*"と"*Enclosure Firmware Management*"を選択してください。詳細については、HPSUM 8.0.0ユーザーガイドを参照してください。

CAC

- CACモードのSSHでは、TelnetおよびXML応答プロトコルは無効になります。

- リンクされたエンクロージャーがCACモードになっている場合、リンクされたエンクロージャーのログインは動作しません。
- サービスアカウントの詳細を正確に指定しないと、証明書を使用したLDAPユーザーのログインは失敗します。
- CACの使用を開始する前にリカバリプランを立てることを強くお勧めします。 OA設定で問題が起こった場合、OAをシリアルポートまたはInsight Displayパネルおよび USB KEYからリカバリできる場合があります。いずれの方法もOAへの物理アクセスが必要です。 ただし、LCD PINが設定されている(または忘れた)場合、およびローカルアカウントが無効になっているかCACが正しく設定されていない場合、リカバリする唯一の方法はシリアルポート経由です。OAの復旧が必要な最も一般的な状況を2つ挙げると、LDAPが無効なローカルアカウントで誤って設定されている場合と、CACが証明書にアクセスしないよう設定されている場合です。

設定可能なSSHポート番号

スタンバイOAが4.85未満のファームウェアバージョンを実行していて、アクティブOAのファームウェア同期機能を使用してファームウェアバージョンが4.85以上に更新した場合、ファームウェアのアップデートおよびスタンバイOAの再起動後、SSHポートは構成されたポート番号で開きません。回避策は、スタンバイOAを再起動することです。SSHポートは、次回起動時に設定されたポートで開きます。SSH ポートがアクティブOAのデフォルトポート22で構成されている場合は、この問題が発生しません。

拡張

Onboard Administrator 4.85は、以下の機能強化に対するサポートを提供します:

ハードウェアの追加

- HPE D2500sb Storage Blade

特徴**: 追加と変更**

全般

- Onboard AdministratorがSNMPエンジンIDとして、IPv6 アドレスを構成できるように拡張されました。
- Onboard Administrator が SSH ポート番号を定義するユーザーを構成できるように拡張されました。これにより、ユーザーはデフォルトのSSHポート22ではなく非標準のSSHポートを設定できます。

セキュリティ

一般的なデータ保護要件(GDPR)サポートは、HPE Embeddedリモートサポートソリューション用のOnboard Administratorに追加されています。HPEパスポートのユーザー名は暗号化された形式で保存されます。

ファームウェア - Lights-Outマネジメント

先頭

オンラインROMフラッシュコンポーネント for Linux - HPE Integrated Lights-Out 4

バージョン: 2.61 **(推奨)**
ファイル名: CP036949.scexe; RPMS/i386/firmware-ilo4-2.61-1.1.i386.rpm

重要な注意！

IPv6ネットワーク通信(専用ネットワーク接続のみ)
サポートされているネットワークの機能
IPv6静的アドレス割り当て
IPv6 SLAACアドレス割り当て
IPv6スタティックルート割り当て
IPv6静的デフォルトゲートウェイ入力
DHCPv6ステートフルアドレス割り当て
DHCPv6ステートレスDNS、ドメイン名、およびNTP設定
統合リモートコンソール
OAシングルサインオン
HP-SIMシングルサインオン
Webサーバー
SSHサーバー

SNTPクライアント
DDNSクライアント
RIBCL over IPv6
SNMP
アラートメール
リモートSyslog
WinDBGサポート
IPv6接続を経由したCPQLOCFGおよびHPLOMIG
スクリプト化可能な仮想メディア
CLI/RIBCL Key Import over IPv6
LDAPおよびKerberos over IPv6を使用した認証
iLO連携

本リリースにおいてIPv6によりサポートされないネットワークの機能

共有ネットワークポート接続経由のIPv6
IPMI
NETBIOS-WINS
Enterprise Secure Key Manager(ESKM)サポート
組み込みリモートサポート (ERS)

事前要件

最良のパフォーマンスを得るには、次のバージョン以上のiLOユーティリティを
お勧めします。

- RESTfulインターフェイスツール(iLOREST)2.3
- HPQLOCFG v5.2
- Lights-Out XMLスクリプティングサンプルバンドル5.10.0
- HPONCFG Windows 5.2.0
- HPONCFG Linux 5.3.0 (A)
- LOCFG v5.10.0
- HPLOMIG 5.2.0

修正

このバージョンでは以下の問題が解決されます。

- サーバーがMicroSDカードから起動するときに断続的な起動の失敗が発生しました。
- 現在の日付の読み取れないデータがある可能性があるAHSダウンロードの問題を修正しました。
- iLO Web GUIセッションが、タイムアウト時間の最後にログオフしない可能性があります。
- AHSビューアーに電源装置ベイに関する誤った情報が表示されます。
- GUIのアクセス設定ページのライセンスハイパーリンクをクリックすると、"ページが見つかりません"と表示されます。
- iLOを出荷時のデフォルト設定に戻した後にiLO CLIにログインできず、追加のiLOリセットが必要になります。
- 特定の特殊文字を使用しているユーザーのRESTインターフェイスセッションを削除できません。
- SNMPは、一定の期間応答しなくなる場合があります。

セキュリティ:

最新のセキュリティ報告書と脆弱性については、次のサイトを参照してください:
https://support.hpe.com/hpesc/public/home

セキュリティ報告書:

- HPESBHF03866

セキュリティに関するベストプラクティス

最新のセキュリティベストプラクティスについては、次のHPE Integrated Lights-Outセキュリティ技術概要を参照してください。
http://www.hpe.com/support/iLO4_security_ja

拡張

なし

オンラインROMフラッシュコンポーネント for Linux - HPE Integrated Lights-Out 5

バージョン: 1.35 **(推奨)**
ファイル名: CP036661.scexe; RPMS/x86_64/firmware-ilo5-1.35-1.1.x86_64.compsig; RPMS/x86_64/firmware-ilo5-1.35-1.1.x86_64.rpm

重要な注意！

IPv6ネットワーク通信(専用ネットワーク接続のみ)
サポートされているネットワークの機能
IPv6静的アドレス割り当て
IPv6 SLAACアドレス割り当て
IPv6スタティックルート割り当て
IPv6静的デフォルトゲートウェイ入力
DHCPv6ステートフルアドレス割り当て
DHCPv6ステートレスDNS、ドメイン名、およびNTP設定
統合リモートコンソール
OAシングルサインオン
HP-SIMシングルサインオン
Webサーバー
SSHサーバー
SNTPクライアント
DDNSクライアント
RIBCL over IPv6
SNMP
アラートメール
リモートSyslog
WinDBGサポート
HPONCFG/HPLOMIG over IPv6接続
スクリプト化可能な仮想メディア
CLI/RIBCL Key Import over IPv6
LDAPおよびKerberos over IPv6を使用した認証
iLO連携
本リリースにおいてIPv6によりサポートされないネットワークの機能
共有ネットワークポート接続経由のIPv6
IPMI
NETBIOS-WINS
Enterprise Secure Key Manager(ESKM)サポート
組み込みリモートサポート (ERS)

事前要件

最良のパフォーマンスを得るには、次のバージョン以上のiLOユーティリティを
お勧めします。

- RESTfulインターフェイスツール(iLOREST)2.3
- HPQLOCFG v5.2
- Lights-Out XMLスクリプティングサンプルバンドル5.10.0
- HPONCFG Windows 5.2.0
- HPONCFG Linux 5.3.0
- LOCFG v5.10.0
- HPLOMIG 5.2.0

注記:iLO高セキュリティ、FIPSおよびCNSAのセキュリティ状態をサポートするには、アップデートされたユーティリティおよびシステムライブラリーが必要です。
HPONCFG Windowsユーティリティ
は、CNSAのセキュリティ状態を現在サポートしていません。

修正

このバージョンでは以下の問題が解決されます。

- 報告された不適切なSmartアレイエラーの修正。キャッシュモジュールボードのバックアップ電源が故障しました。
- 仮想メディアを取り出した後にiLOが応答しなくなる問題を修正しました。

セキュリティの修正:

最新のセキュリティ報告書と脆弱性については、次のサイトを参照してください:
https://support.hpe.com/hpesc/public/home

- セキュリティ情報 HPESBHF03866

セキュリティに関するベストプラクティス

最新のセキュリティベストプラクティスについては、次のHPE Integrated Lights-Out 5セキュリティ技術概要を参照してください。
http://www.hpe.com/support/ilo5-security-en

拡張

このバージョンは、以下の機能と改善を追加しました。

- VGAポート検出オーバーライド - システムのビデオポートに接続されているデバイスの検出方法を制御します。動的検出によってシステムが異常なポート電圧から保護されます。この設定はデフォルトで有効になっています。ディスプレイ、KVMコンセントレーター、またはアクティブなドングルへのビデオ出力がない場合のトラブルシューティングでこの設定を使用できます。
- iLO RESTful APIを介したDHCPクライアントIDオーバーライド

オンラインROMフラッシュコンポーネント for VMware ESXi -HPE Integrated Lights-Out 4

バージョン: 2.61 **(推奨)**
ファイル名: CP036950.compsig; CP036950.zip

重要な注意！

IPv6ネットワーク通信(専用ネットワーク接続のみ)
サポートされているネットワークの機能
IPv6静的アドレス割り当て
IPv6 SLAACアドレス割り当て
IPv6静的ルート割り当て
IPv6静的デフォルトゲートウェイ入力
DHCPv6ステートフルアドレス割り当て
DHCPv6ステートレスDNS、ドメイン名、およびNTP設定
Integrated Remote Console (統合リモートコンソール)。
OAシングルサインオン
HP-SIMシングルサインオン
Webサーバー
SSHサーバー
SNTPクライアント
DDNSクライアント
RIBCL over IPv6
SNMP
アラートメール

リモートSyslog
WinDBGサポート
IPv6接続を経由したCPQLOCFGおよびHPLOMIG
スクリプト化可能な仮想メディア
CLI/RIBCL Key Import over IPv6
LDAPおよびKerberos over IPv6を使用した認証
iLO連携

本リリースにおいてIPv6によりサポートされないネットワークの機能

共有ネットワークポート接続経由のIPv6
IPMI
NETBIOS-WINS
Enterprise Secure Key Manager(ESKM)サポート
組み込みリモートサポート (ERS)

事前要件

最良のパフォーマンスを得るには、次のバージョン以上のiLOユーティリティを
お勧めします。

- RESTfulインターフェイスツール(iLOREST)2.3
- HPQLOCFG v5.2
- Lights-Out XMLスクリプティングサンプルバンドル5.10.0
- HPONCFG Windows 5.2.0
- HPONCFG Linux 5.3.0 (A)
- LOCFG v5.10.0
- HPLOMIG 5.2.0

修正

このバージョンでは以下の問題が解決されます。

- サーバーがMicroSDカードから起動するときに断続的な起動の失敗が発生しました。
- 現在の日付の読み取れないデータがある可能性があるAHSダウンロードの問題を修正しました。
- iLO Web GUIセッションが、タイムアウト時間の最後にログオフしない可能性があります。
- AHSビューアーに電源装置ベイに関する誤った情報が表示されます。
- GUIのアクセス設定ページのライセンスハイパーリンクをクリックすると、"ページが見つかりません"と表示されます。
- iLOを出荷時のデフォルト設定に戻した後にiLO CLIにログインできず、追加のiLOリセットが必要になります。
- 特定の特殊文字を使用しているユーザーのRESTインターフェイスセッションを削除できません。
- SNMPは、一定の期間応答しなくなる場合があります。

セキュリティ:

最新のセキュリティ報告書と脆弱性については、次のサイトを参照してください:
https://support.hpe.com/hpesc/public/home

セキュリティ報告書:

- HPESBHF03866

セキュリティに関するベストプラクティス

最新のセキュリティベストプラクティスについては、次のHPE Integrated Lights-Outセキュリティ技術概要を参照してください。
http://www.hpe.com/support/iLO4_security_ja

拡張

なし

オンラインROMフラッシュコンポーネント for Windows x64- HPE Integrated Lights-Out 4

バージョン: 2.61 **(推奨)**
ファイル名: cp036948.exe

重要な注意！

IPv6ネットワーク通信(専用ネットワーク接続のみ)
サポートされているネットワークの機能
IPv6静的アドレス割り当て
IPv6 SLAACアドレス割り当て
IPv6静的ルート割り当て
IPv6静的デフォルトゲートウェイ入力
DHCPv6ステートフルアドレス割り当て
DHCPv6ステートレスDNS、ドメイン名、およびNTP設定
Integrated Remote Console (統合リモートコンソール)。
OAシングルサインオン
HP-SIMシングルサインオン
Webサーバー
SSHサーバー
SNTPクライアント
DDNSクライアント
RIBCL over IPv6
SNMP
アラートメール
リモートSyslog
WinDBGサポート
IPv6接続を経由したCPQLOCFGおよびHPLOMIG
スクリプト化可能な仮想メディア
CLI/RIBCL Key Import over IPv6
LDAPおよびKerberos over IPv6を使用した認証
iLO連携
本リリースにおいてIPv6によりサポートされないネットワークの機能
共有ネットワークポート接続経由のIPv6
IPMI
NETBIOS-WINS
Enterprise Secure Key Manager(ESKM)サポート
組み込みリモートサポート (ERS)

事前要件

最良のパフォーマンスを得るには、次のバージョン以上のiLOユーティリティを
お勧めします。

- RESTfulインターフェイスツール(iLOREST)2.3
- HPQLOCFG v5.2
- Lights-Out XMLスクリプティングサンプルバンドル5.10.0
- HPONCFG Windows 5.2.0
- HPONCFG Linux 5.3.0 (A)
- LOCFG v5.10.0
- HPLOMIG 5.2.0

修正

このバージョンでは以下の問題が解決されます。

- サーバーがMicroSDカードから起動するときに断続的な起動の失敗が発生しました。
- 現在の日付の読み取れないデータがある可能性があるAHSダウンロードの問題を修正しました。
- iLO Web GUIセッションが、タイムアウト時間の最後にログオフしない可能性があります。
- AHSビューアーに電源装置ベイに関する誤った情報が表示されます。

- GUIのアクセス設定ページのライセンスハイパーリンクをクリックすると、"ページが見つかりません"と表示されます。
- iLOを出荷時のデフォルト設定に戻した後にiLO CLIにログインできず、追加のiLOリセットが必要になります。
- 特定の特殊文字を使用しているユーザーのRESTインターフェイスセッションを削除できません。
- SNMPは、一定の期間応答しなくなる場合があります。

セキュリティ:

最新のセキュリティ報告書と脆弱性については、次のサイトを参照してください:
https://support.hpe.com/hpesc/public/home

セキュリティ報告書:

- HPESBHF03866

セキュリティに関するベストプラクティス

最新のセキュリティベストプラクティスについては、次のHPE Integrated Lights-Outセキュリティ技術概要を参照してください。
http://www.hpe.com/support/iLO4_security_ja

拡張

なし

オンラインROMフラッシュコンポーネント for Windows x64- HPE Integrated Lights-Out 5

バージョン: 1.35 **(推奨)**
ファイル名: cp036662.compsig; cp036662.exe

重要な注意！

IPv6ネットワーク通信(専用ネットワーク接続のみ)
サポートされているネットワークの機能
IPv6静的アドレス割り当て
IPv6 SLAACアドレス割り当て
IPv6スタティックルート割り当て
IPv6静的デフォルトゲートウェイ入力
DHCPv6ステートフルアドレス割り当て
DHCPv6ステートレスDNS、ドメイン名、およびNTP設定
統合リモートコンソール
OAシングルサインオン
HP-SIMシングルサインオン
Webサーバー
SSHサーバー
SNTPクライアント
DDNSクライアント
RIBCL over IPv6
SNMP
アラートメール
リモートSyslog
WinDBGサポート
HPONCFG/HPLOMIG over IPv6接続
スクリプト化可能な仮想メディア
CLI/RIBCL Key Import over IPv6
LDAPおよびKerberos over IPv6を使用した認証
iLO連携
本リリースにおいてIPv6によりサポートされないネットワークの機能
共有ネットワークポート接続経由のIPv6
IPMI

NETBIOS-WINS
Enterprise Secure Key Manager(ESKM)サポート
組み込みリモートサポート (ERS)

事前要件

最良のパフォーマンスを得るには、次のバージョン以上のiLOユーティリティを
お勧めします。

- RESTfulインターフェイスツール(iLOREST)2.3
- HPQLOCFG v5.2
- Lights-Out XMLスクリプティングサンプルバンドル5.10.0
- HPONCFG Windows 5.2.0
- HPONCFG Linux 5.3.0
- LOCFG v5.10.0
- HPLOMIG 5.2.0

注記:iLO高セキュリティ、FIPSおよびCNSAのセキュリティ状態をサポートするには、アップデートされたユーティリティおよびシステムライブラリーが必要です。
HPONCFG Windowsユーティリティ
は、CNSAのセキュリティ状態を現在サポートしていません。

修正

このバージョンでは以下の問題が解決されます。

- 報告された不適切なSmartアレイエラーの修正。キャッシュモジュールボードのバックアップ電源が故障しました。
- 仮想メディアを取り出した後にiLOが応答しなくなる問題を修正しました。

セキュリティの修正:

最新のセキュリティ報告書と脆弱性については、次のサイトを参照してください:
https://support.hpe.com/hpesc/public/home

- セキュリティ情報 HPESBHF03866

セキュリティに関するベストプラクティス

最新のセキュリティベストプラクティスについては、次のHPE Integrated Lights-Out 5セキュリティ技術概要を参照してください。
http://www.hpe.com/support/ilo5-security-en

拡張

このバージョンは、以下の機能と改善を追加しました。

- VGAポート検出オーバーライド - システムのビデオポートに接続されているデバイスの検出方法を制御します。動的検出によってシステムが異常なポート電圧から保護されます。この設定はデフォルトで有効になっています。ディスプレイ、KVMコンセントレーター、またはアクティブなドングルへのビデオ出力がない場合のトラブルシューティングでこの設定を使用できます。
- iLO RESTful APIを介したDHCPクライアントIDオーバーライド

オンラインROMフラッシュファームウェアパッケージ - HPE Integrated Lights-Out 5

バージョン: 1.35 **(推奨)**
ファイル名: ilo5_135.fwpkg

重要な注意！

IPv6ネットワーク通信(専用ネットワーク接続のみ)
サポートされているネットワークの機能

IPv6静的アドレス割り当て
IPv6 SLAACアドレス割り当て
IPv6スタティックルート割り当て
IPv6静的デフォルトゲートウェイ入力
DHCPv6ステートフルアドレス割り当て
DHCPv6ステートレスDNS、ドメイン名、およびNTP設定
統合リモートコンソール
OAシングルサインオン
HP-SIMシングルサインオン
Webサーバー
SSHサーバー
SNTPクライアント
DDNSクライアント
RIBCL over IPv6
SNMP
アラートメール
リモートSyslog
WinDBGサポート
HPONCFG/HPLOMIG over IPv6接続
スクリプト化可能な仮想メディア
CLI/RIBCL Key Import over IPv6
LDAPおよびKerberos over IPv6を使用した認証
iLO連携

本リリースにおいてIPv6によりサポートされないネットワークの機能
共有ネットワークポート接続経由のIPv6
IPMI
NETBIOS-WINS
Enterprise Secure Key Manager(ESKM)サポート
組み込みリモートサポート (ERS)

事前要件

最良のパフォーマンスを得るには、次のバージョン以上のiLOユーティリティを
お勧めします。

- RESTfulインターフェイスツール(iLOREST)2.3
- HPQLOCFG v5.2
- Lights-Out XMLスクリプティングサンプルバンドル5.10.0
- HPONCFG Windows 5.2.0
- HPONCFG Linux 5.3.0
- LOCFG v5.10.0
- HPLOMIG 5.2.0

注記:iLO高セキュリティ、FIPSおよびCNSAのセキュリティ状態をサポートするには、アップデートされたユーティリティおよびシステムライブラリーが必要です。
HPONCFG Windowsユーティリティ
は、CNSAのセキュリティ状態を現在サポートしていません。

修正

このバージョンでは以下の問題が解決されます。

- 報告された不適切なSmartアレイエラーの修正。キャッシュモジュールボードのバックアップ電源が故障しました。
- 仮想メディアを取り出した後にiLOが応答しなくなる問題を修正しました。

セキュリティの修正:

最新のセキュリティ報告書と脆弱性については、次のサイトを参照してください:
https://support.hpe.com/hpesc/public/home

- セキュリティ情報 HPESBHF03866

セキュリティに関するベストプラクティス

最新のセキュリティベストプラクティスについては、次のHPE Integrated Lights-Out 5セキュリティ技術概要を参照してください。
http://www.hpe.com/support/ilo5-security-en

拡張

このバージョンは、以下の機能と改善を追加しました。

- VGAポート検出オーバーライド - システムのビデオポートに接続されているデバイスの検出方法を制御します。動的検出によってシステムが異常なポート電圧から保護されます。この設定はデフォルトで有効になっています。ディスプレイ、KVMコンセントレーター、またはアクティブなドングルへのビデオ出力がない場合のトラブルシューティングでこの設定を使用できます。
- iLO RESTful APIを介したDHCPクライアントIDオーバーライド

ファームウェア - ネットワーク

先頭

HPE Broadcom NetXtreme-Eオンライン ファームウェアアップグレードユーティリティ for VMware

バージョン: 5.5.0 **(オプション)**
ファイル名: CP035379.compsig; CP035379.zip

重要な注意！

このファームウェアとともに使用する場合は、*HPE Broadcom NetXtreme-E Drivers for VMware*、バージョン2018.09.00以降を推奨しています。

このソフトウェアパッケージには、下記のファームウェアバージョンを含むNVMイメージバージョン212.0.103001が含まれています:

NIC	Bootcodeバージョン	NCSIバージョン	MBAバージョン	UEFIバージョン	CCMバージョン	RoCEバージョン
HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター	212.0.102.0	212.0.96.0	212.0.92.0	212.0.103.1	212.0.92.0	212.0.103.0
HPE Ethernet 10Gb 2ポート 535Tアダプター						
HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター						
HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター						

事前要件

この製品では、ファームウェアをアップデートする前に、使用するデバイスおよびオペレーティングシステム用の適切なドライバーがインストールされている必要があります。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-Eオンラインファームウェアアップグレードユーティリティ for Linux x86_64

バージョン: 1.3.56 **(オプション)**
ファイル名: firmware-nic-bcm-nxe-1.3.56-1.1.x86_64.compsig; firmware-nic-bcm-nxe-1.3.56-1.1.x86_64.rpm

重要な注意！

このファームウェアとともに使用する場合は、*HPE Broadcom NetXtreme-E Drivers for Linux*、バージョン1.9.1-212.0.99.0以降を推奨しています。

事前要件

このパッケージには、ご使用のネットワークアダプターのための適切なドライバーがインストールされ、ファームウェアを更新する前にすべてのイーサーネットポートがアップ(*ifup ethX* または*ifconfig ethX up*)している必要があります。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NetXtreme-Eオンラインファームウェアアップグレードユーティリティ for Windows Server x64 Edition

バージョン: 5.1.3.0 **(オプション)**
ファイル名: cp034397.compsig; cp034397.exe

重要な注意！

このファームウェアとともに使用する場合は、*HPE Broadcom NetXtreme-E Driver for Windows*、バージョン212.0.89.0以降を推奨しています。

事前要件

この製品では、ファームウェアをアップデートする前に、使用するデバイスおよびオペレーティングシステム用の適切なドライバーがインストールされている必要があります。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 535FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 535Tアダプター
- HPE Ethernet 10/25Gb 2ポート 631FLR-SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 631SFP28アダプター

HPE Broadcom NX1オンライン ファームウェアアップグレードユーティリティ for VMware

バージョン: 1.22.1 **(オプション)**
ファイル名: CP035378.compsig; CP035378.zip

重要な注意！

HPEは、このファームウェア用に *HP Broadcom tg3 Ethernet*ドライバー *for VMware*、バージョン2018.09.00またはそれ以降を推奨します。

このソフトウェアパッケージには、下記のファームウェアバージョンを含むコンボイメージv20.12.41が含まれています:

NIC	ブートコードバージョン	PXEバージョン	NCSIバージョン	UEFIバージョン	CCMバージョン
HP Ethernet 1Gb 2ポート 330iアダプター(22BD)	2.10	20.6.50	1.4.22	20.12.2	212.0.92.0
HP Ethernet 1Gb 4ポート 331iアダプター(22BE) HP Ethernet 1Gb 4ポート 331FLRアダプター HP Ethernet 1Gb 4ポート 331Tアダプター	1.46	20.6.50	1.4.22	20.12.2	212.0.92.0
HP Ethernet 1Gb 2ポート 332iアダプター(2133)	1.39	20.6.50	1.4.22	n/a	212.0.92.0
HP Ethernet 1Gb 2ポート 332iアダプター(22E8) HP Ethernet 1Gb 2ポート 332Tアダプター	1.39	20.6.50	1.4.22	20.12.2	212.0.92.0

事前要件

この製品では、ファームウェアをアップデートする前に、使用するデバイスおよびオペレーティングシステム用の適切なドライバーがインストールされている必要があります。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 330iアダプター(22BD)
- HP Ethernet 1Gb 4ポート 331iアダプター(22BE)
- HPE Ethernet 1Gb 4ポート 331FLRアダプター
- HPE Ethernet 1Gb 4ポート 331Tアダプター
- HP Ethernet 1Gb 2ポート 332iアダプター(2133)
- HP Ethernet 1Gb 2ポート 332iアダプター(22E8)
- HPE Ethernet 1Gb 2ポート 332Tアダプター

HPE Broadcom NX1オンラインファームウェアアップグレードユーティリティ for Linux x86_64

バージョン: 2.21.58 **(オプション)**
ファイル名: firmware-nic-broadcom-2.21.58-1.1.x86_64.compsig; firmware-nic-broadcom-2.21.58-1.1.x86_64.rpm

重要な注意！

このファームウェアとともに使用する場合は、*HPE Broadcom tg3 Ethernet Drivers*、バージョン3.137w-3以降を推奨しています。

事前要件

このパッケージには、ご使用のネットワークアダプターのための適切なドライバーがインストールされ、ファームウェアを更新する前にすべてのイーサーネットポートがアップ(*ifup ethX* または*ifconfig ethX up*)している必要があります。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 330iアダプター(22BD)
- HP Ethernet 1Gb 4ポート 331iアダプター(22BE)
- HPE Ethernet 1Gb 4ポート 331FLRアダプター
- HPE Ethernet 1Gb 4ポート 331Tアダプター
- HP Ethernet 1Gb 2ポート 332iアダプター(2133)
- HP Ethernet 1Gb 2ポート 332iアダプター(22E8)
- HPE Ethernet 1Gb 2ポート 332Tアダプター

HPE Broadcom NX1オンラインファームウェアアップグレードユーティリティ for Windows Server x64 Edition

バージョン: 5.1.3.0 **(オプション)**
ファイル名: cp034766.compsig; cp034766.exe

重要な注意！

このファームウェアとともに使用する場合は、*HPE Broadcom 1Gb Driver for Windows Server x64 Edition*、バージョン212.0.0.0以降を推奨しています。

事前要件

この製品では、ファームウェアをアップデートする前に、使用するデバイスおよびオペレーティングシステム用の適切なドライバーがインストールされている必要があります。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 330iアダプター(22BD)
- HP Ethernet 1Gb 4ポート 331iアダプター(22BE)
- HPE Ethernet 1Gb 4ポート 331FLRアダプター
- HPE Ethernet 1Gb 4ポート 331Tアダプター
- HP Ethernet 1Gb 2ポート 332iアダプター(2133)
- HP Ethernet 1Gb 2ポート 332iアダプター(22E8)
- HPE Ethernet 1Gb 2ポート 332Tアダプター

HPE Firmware Flash for Emulex Converged Network Adapters for Linux (x64)

バージョン: 2018.09.01 **(推奨)**
ファイル名: RPMS/x86_64/firmware-cna-emulex-2018.09.01-1.5.x86_64.compsig; RPMS/x86_64/firmware-cna-emulex-2018.09.01-1.5.x86_64.rpm

重要な注意！

リリースノート:

HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

ファームウェアアップデートは、インボックスまたはOut of Box(OOB)ドライバーを使用して実行できます。サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

OOB NICドライバーは、http://www.hpe.com/servers/spp/downloadのService Pack for ProLiant(SPP)から入手できます。

追加の要件:

ファームウェアアップデートキットのインストール前にターゲット環境にlibsysfsまたはsysfsutilsパッケージをインストールしておく必要があります。存在していない場合、libsysfsまたはsysfsutilsパッケージはオペレーティングシステムのインストールメディアから取得することができます。

コンポーネントがEmulex HBA/CNAを検出できるようにするために32-bit netlink library (libnl.so) がインストールされている環境が必要です
フラッシュエンジンを動作させるためにsyslogデーモンが実行されている環境が必要です

注記:FCoE/iSCSIプロトコルをサポートするデバイス上でプロトコルを有効にするには、適切なEmulex FCoE/iSCSIドライバーをインストールしてください。 また、FCoEプロトコルは、HPE Emulexイネーブルメントキットがインストールされている必要があります。 また、ドライバーおよびイネーブルメントキットは、http://www.hpe.com/servers/spp/downloadのService Pack for ProLiant(SPP)から入手できます。

イネーブルメントキットは、OSインストールメディアからlibHBAAPIパッケージをインストールしたターゲット環境を必要とします。

FCoEドライバーキットをインストールし、再起動してからイネーブルメントキットをインストールします。

拡張

ファイバーチャネルおよびコンバージドネットワークアダプターをアップデートする別々のコンポーネントがあります。 これは、コンバージドネットワークアダプターアップデートコンポーネントです。

CNA (XE100シリーズ)ファームウェアをアップデートしました

ファームウェア

含まれるもの:
CNA (XE100シリーズ)ファームウェア12.0.1110.11

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HP Ethernet 10Gb 2ポート 557SFP+ アダプター
- HPE StoreFabric CN1200E-Tアダプター

HPE Firmware Flash for Emulex Converged Network Adapters for Windows (x64)

バージョン: 2018.06.01 **(推奨)**
ファイル名: cp034215.compsig; cp034215.exe

重要な注意！

リリースノート:

HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

ファームウェアアップデートは、インボックスまたはOut of Box(OOB)ドライバーを使用して実行できます。 サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

このファームウェアコンポーネントが開発用のSUMで識別される前に、HPEで提供しているEmulex NICドライバーをインストールする必要があります。最新のドライバーは、HPE.com Webサイト:http://www.hpe.com/から入手できます。

CoE/iSCSI OOBドライバーおよびFCoEイネーブルメントキットは、http://www.hpe.com/servers/spp/downloadのService Pack for ProLiant(SPP)から入手できます。

拡張

ファイバーチャネルおよびコンバージドネットワークアダプターをアップデートする別々のコンポーネントがあります。 これは、コンバージドネットワークアダプターアップデートコンポーネントです。

CNA (XE100シリーズ)ファームウェアをアップデートしました

ファームウェア

含まれるもの:
CNA (XE100シリーズ)ファームウェア12.0.1110.11

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HPE StoreFabric CN1200E-Tアダプター

HPE Intelオンライン ファームウェアアップグレードユーティリティ for VMware

バージョン: 3.8.0 **(オプション)**
ファイル名: CP035380.compsig; CP035380.zip

重要な注意！

HPEは、このファームウェアで使用するために、ご使用のデバイスに適用可能な次のドライバーの少なくとも1つをお勧めします:

- *HPE Intel igbn*ドライバー*for VMware*、バージョン2018.09.00 以降
- *HPE Intel ixgben*ドライバー*for VMware*、バージョン2018.09.00以降
- *HPE Intel i40en*ドライバー*for VMware*、バージョン2018.09.00以降

このソフトウェアパッケージは、以下にリストされるサポートされるネットワークアダプターの次のファームウェアのバージョンを含みます:

NIC	EEPROM/NVMバージョン	OROMバージョン	シングルNVMバージョン
HP Ethernet 1Gb 2ポート 361iアダプター	80000CD5	1.1904.0	N/A
HP Ethernet 1Gb 2ポート 361Tアダプター	80000F91	1.1904.0	N/A
HP Ethernet 1Gb 2ポート 363iアダプター	80000D00	1.1904.0	N/A
HP Ethernet 1Gb 1-port 364i アダプター	80000BEE	1.1904.0	N/A
HP Ethernet 1Gb 4ポート 366iアダプター	80000E24	1.1904.0	N/A
HPE Ethernet 1Gb 4ポート 366i通信ボード	80000EBF	1.1904.0	N/A
HP Ethernet 1Gb 4ポート 366FLRアダプター	80000F44	1.1904.0	N/A
HP Ethernet 1Gb 4ポート 366Mアダプター	80000DA9	1.1904.0	N/A
HP Ethernet 1Gb 4ポート 366Tアダプター	80000E81	1.1904.0	N/A
HPE Ethernet 1Gb 2ポート 368i アダプター	80001111	1.1904.0	N/A
HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター	80001110	1.1904.0	N/A
HPE Ethernet 1Gb 4ポート 369i アダプター	80001112	1.1904.0	N/A
HP Ethernet 10Gb 2ポート 560FLBアダプター	800008F0	1.1904.0	N/A
HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター	80000838	1.1904.0	N/A
HP Ethernet 10Gb 2ポート 560M アダプター	8000083D	1.1904.0	N/A
HPE Ethernet 10Gb 2ポート 560SFP+アダプター	80000835	1.1904.0	N/A

NIC	EEPROM/NVMバージョン	OROMバージョン	シングルNVMバージョン
HP Ethernet 10Gb 2ポート 561FLR-Tアダプター	800005B6	1.1904.0	N/A
HP Ethernet 10Gb 2ポート 561Tアダプター	80000636	1.1904.0	N/A
HPE Ethernet 10Gb 2ポート 568iアダプター	80001113	1.1904.0	N/A
HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター	80001110	1.1904.0	N/A
HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター	80001110	1.1904.0	N/A
HPE Ethernet 10Gb 2ポート 563i アダプター	800035C0	1.1375.0	N/A
HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター	800038C9	1.1904.0	10.3.5
HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター	80000BF1	1.1904.0	10.3.5
HPE Ethernet 10Gb 2ポート 562SFP+アダプター	800038C8	1.1904.0	10.3.5
HPE Ethernet 10Gb 2ポート 562Tアダプター	80000BF0	1.1904.0	10.3.5

コンボイメージv1.1904.0は以下を含みます:Boot Agent: 1GbE - v1.5.85、10GbE - v2.4.16、40GbE - v1.0.66 &UEFIドライバー:1GbE - v8.3.10、10GbE - v6.7.10、40GbE - v3.0.11

コンボイメージv1.1375.0は以下を含みます:Boot Agent: 1GbE - v1.5.72、10GbE - v2.3.46、40GbE - v1.0.21 &UEFIドライバー: 1GbE - v6.9.13、10GbE - v5.0.20、40GbE - v1.5.14。

シングルNVMバージョンは、以前に使用されていたバージョンEEPROM/NVMまたはOROMバージョンの代わりに統合されたバージョンを表す新しいファームウェア形式です。

事前要件

この製品では、ファームウェアをアップデートする前に、使用するデバイスおよびオペレーティングシステム用の適切なドライバーがインストールされている必要があります。

サポートしているデバイスおよび機能

このパッケージは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 361iアダプター
- HP Ethernet 1Gb 2-port 361Tアダプター
- HP Ethernet 1Gb 2ポート 363iアダプター
- HP Ethernet 1Gb 1-port 364i アダプター
- HP Ethernet 1Gb 4-port 366FLRアダプター
- HP Ethernet 1Gb 4ポート 366iアダプター
- HPE Ethernet 1Gb 4-port 366i通信ボード
- HP Ethernet 1Gb 4ポート 366Mアダプター
- HP Ethernet 1Gb 4ポート 366Tアダプター
- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2-port 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター

- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2-port 563i アダプター
- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター

HPE Intelオンラインファームウェアアップグレードユーティリティ for Linux x86_64

バージョン: 1.15.56 **(オプション)**
ファイル名: firmware-nic-intel-1.15.56-1.1.x86_64.compsig; firmware-nic-intel-1.15.56-1.1.x86_64.rpm

重要な注意！

HPEは、このファームウェアで使用するために、ご使用のデバイスに適用可能な次のドライバーの少なくとも1つをお勧めします:

- Linux用HPE Intel igbドライバー、バージョン5.3.5.15以降
- Linux用HPE Intel ixgbeドライバー、バージョン5.3.5.1以降
- Linux用HPE Intel i40eドライバー、バージョン2.4.6.1以降

事前要件

この製品では、ファームウェアをアップデートする前に、使用するデバイスおよびオペレーティングシステム用の適切なドライバーがインストールされている必要があります。

サポートしているデバイスおよび機能

このパッケージは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 361iアダプター
- HP Ethernet 1Gb 2-port 361Tアダプター
- HP Ethernet 1Gb 2ポート 363iアダプター
- HP Ethernet 1Gb 1-port 364i アダプター
- HP Ethernet 1Gb 4-port 366FLRアダプター
- HP Ethernet 1Gb 4ポート 366iアダプター
- HPE Ethernet 1Gb 4-port 366i通信ボード
- HP Ethernet 1Gb 4ポート 366Mアダプター
- HP Ethernet 1Gb 4ポート 366Tアダプター
- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2-port 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター
- HPE Ethernet 10Gb 2-port 563i アダプター
- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 10Gb 2ポート 562Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター

HPE Intelオンラインファームウェアアップグレードユーティリティ for Windows Server x64 Edition

バージョン: 5.1.3.0 **(オプション)**
ファイル名: cp034074.compsig; cp034074.exe

重要な注意！

HPEは、このファームウェアで使用するために、ご使用のデバイスに適用可能な次の少なくとも1つをお勧めします:

- *HPE Intel E1R Driver for Windows Server 2012*、バージョン12.14.8.0以降
- *HPE Intel E1R Driver for Windows Server 2016*、バージョン12.15.184.0(B)以降
- *HPE Intel ixn Driver for Windows Server 2012*、バージョン3.14.76.0以降
- *HPE Intel ixn Driver for Windows Server 2016*、バージョン4.1.74.0以降
- *HPE Intel ixs Driver for Windows Server 2012 R2*、バージョン3.14.75.0以降
- *HPE Intel ixs Driver for Windows Server 2016*、バージョン4.1.74.0以降
- *HPE Intel ixt Driver for Windows Server 2012*、バージョン3.14.76.0以降
- *HPE Intel ixt Driver for Windows Server 2016*、バージョン4.1.74.0以降
- *HPE Intel i40ea Driver for Windows*、バージョン1.8.94.0以降
- *HPE Intel i40eb Driver for Windows*、バージョン1.8.94.0以降

事前要件

この製品では、ファームウェアをアップデートする前に、使用するデバイスおよびオペレーティングシステム用の適切なドライバーがインストールされている必要があります。

修正

この製品はUEFIモードで動作しているときに、NIC Human Interface Infrastructure(HII)メニューに表示されるNIC VLAN IDの問題を解決します。
この製品は、HPE Ethernet 10Gb 2ポート561Tアダプターが、NICが無効になった後でも引き続きスイッチに接続されているように見えるチーミングの問題に対処しています。
この製品は、HPE Ethernet 10Gb 2ポート560FLBアダプターで見られるリンクの問題とPXEの問題に対処します。
この製品は、HPE Ethernet 1Gb 4ポート366Tアダプターで見られるWOL問題に対処します。

サポートしているデバイスおよび機能

このパッケージは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 361iアダプター
- HP Ethernet 1Gb 2ポート 361Tアダプター
- HP Ethernet 1Gb 2ポート 363iアダプター
- HP Ethernet 1Gb 1-port 364i アダプター
- HP Ethernet 1Gb 4ポート 366FLRアダプター
- HP Ethernet 1Gb 4ポート 366iアダプター
- HPE Ethernet 1Gb 4ポート 366i通信ボード
- HP Ethernet 1Gb 4ポート 366Mアダプター
- HP Ethernet 1Gb 4ポート 366Tアダプター
- HPE Ethernet 1Gb 2ポート 368i アダプター
- HPE Ethernet 1Gb 2ポート 368FLR-MMT アダプター
- HPE Ethernet 1Gb 4ポート 369i アダプター
- HP Ethernet 10Gb 2ポート 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2ポート 561Tアダプター
- HPE Ethernet 10Gb 2ポート 562FLR-SFP+アダプター
- HPE Ethernet 10Gb 2ポート 562FLR-Tアダプター
- HPE Ethernet 10Gb 2ポート 562SFP+アダプター

- HPE Ethernet 10Gb 2ポート 562Tアダプター
- HPE Ethernet 10Gb 2ポート 563i アダプター
- HPE Ethernet 10Gb 2ポート 568iアダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMSFP+アダプター
- HPE Ethernet 10Gb 2ポート 568FLR-MMT アダプター

HPE Mellanox Ethernetアダプター専用のオンラインファームウェアアップグレードユーティリティ(ESXi 6.5)

バージョン: 1.0.3 **(推奨)**
ファイル名: CP034530.compsig; CP034530.zip

重要な注意！

FWバージョン2.42.5000 での既知の問題:

- mlxconfigを使用してcq_timestampを有効または無効にすることはサポートされていません。
- 2つの別個のLEDスキーム(Phy LEDと論理LED)を備えたカードでは、Phy LEDだけが点灯します。つまり、オレンジ色のLEDは、ETHリンクがアイドルモードの間はアクティブではありません。
- SR-IOVセットアップでは、PFがVMに渡されるときにmlxconfigを使用すると、ハイパーバイザーの再起動を必要とします。
- 前のGAにダウングレードするにはサーバーのリブートが必要です。v2.30.8000以降のバージョンから2.30.8000より前のバージョンにダウングレードするには、サーバーのリブートが必要です。サーバーを再起動します。
- ConnectX-3 Ethernet アダプターカードでは、ファームウェア管理ツールによって返されるGUID値とデバイスファームウェアを通してGUIDを読み込むファブリック/ドライバーユーティリティ(例えば、ibstatを使用)によって返される値の間にミスマッチがあります。ユーティリティがMACアドレスから得られた値を返すとき、Mlxburn/flintはGUIDとして0xffffを返します。すべてのドライバー/ファームウェア/ソフトウェアのために、後者の値が使用されるべきです。
- SBRはConnectX®-3アダプターのために最低50msアサートされる必要があります
- Pilot1 SL230で、PCIeリンクは時々Gen3の速度に達しません。
- ドライバーの互換性の問題のため、SR-IOVがVPIカードで有効になっている場合、RH6.3インボックスドライバーがカーネルパニックを引き起こします。
- アドバンストステアリングモードで、MCGごとに8以上のQPを持つ場合、サイドバンド管理接続性が失われることがあります。
- システムBIOSでSR-IOVが無効にされたとき、Linuxカーネルv3.8のUbuntu v12.04.3で、Mellanoxを含むいくつかの製造業者のNICが動作しない可能性があるPCI問題が認識されています。
- MFTツールは、ツール動作が停止を強制された場合にロックされたフラッシュセマフォを残すことがありました。セマフォがロックされていると、ファームウェアはフラッシュにアクセスすることができず、ハングアップします。
- MC2210411-SR4モジュールを使用する場合、ケーブル情報MADは正しくないケーブル情報をレポートします。
- 10C/分以上のスピードで温度が上昇するとGen2が故障します(MT27518A1-FDIR-BVのみ)。
- MT27518A1-FDIR-BVでは10C/分以上のスピードで温度が上昇するとPCIe Gen2リンクが不安定になります。
- Bloomフィルターは、現在サポートされません。
- ファームウェアダウングレードメッセージ ファームウェアv2.11.0000からダウングレードし、MFT 3.0.0-3を使用する場合
- MLNX_OFED-2.0.3でInfiniBandを使用する場合、RM＃DMFSを有効にしないでください
- RM#VPD読み取り専用のフィールドが書き込み可能です。
- SymbolErrorCounterの増加 ポート1 FDRとポート2 40Gを使用してVPIモードで動作すると、エラーカウンターが誤動作して急激に増加します
- デバイスを128Byte CQ/EQストライドに設定するとサイドバンド管理が正常に機能せず、コミュニケーション消失につながります。
- CQおよびEQを異なるストライドサイズに構成することはできません。
- ConnectX-3 Pro VFデバイスIDは、ドライバーの制限のためのConnectX-3 VFデバイスIDと同じように示されます。
- PXE (レガシー)をG9サーバーで稼働中のRSOD。これはPXEブートに失敗し、BIOSがHDDからブートするときにのみ起こります。現在BIOSの修正は保留中です。
- ポートがETHスイッチに接続されているときに、NCSI/IPMIが有効になっている状態でポートプロトコルをETHからIBに変更することは推奨されません。
- IPv6上でのRDPは、現在機能しません。
- Sniffer QP では、"push to that rule"と同等の挿入スキームのあるQPを追加した後に正規のルールを削除できません。
- PCI Physical FunctionごとのBoot Entry Vector (BEV)のみがサポートされているので、最初のポートを無効化すると、二番目のポートも消えてしまいます。

- NICは、56GbEポートリンクのNICポートからケーブルが外れてしまっている場合に、リンクダウンをドライバーに通知しません。
- 100GbE 光ケーブルを使用している場合に、56GbE リンクが起動しません。
- MLNX_OFED v3.3-1.0.0.0を使用している場合、サーバーのリブートが非同期イベントハンドラーから呼ばれたmlx-4_en_get_drvinfo() のカーネルパニックにより、動けなくなることがあります。
- 832298: ibdumpを実行しているとき、ループバックトラフィックがカーネルドライバーにミラーリングされます。
- AHSが誤ったMTUサイズをレポートします
- RM#846523: ifconfigを使用してOSから設定されたMACアドレスがOCBBバッファーに反映されません。

FWバージョン14.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。
- mlxconfigツールが、既存の拡張ROMイメージだけを表示するのでなく、可能なすべての拡張ROMイメージを表示します。
- nic_receive_steering_discard コマンドを実行しているとき、イーサーネットマルチキャストループバックパケットがカウントされません(ローカルループバックパケットでなくても)。
- デュアルポートVHCAが非ネイティブポートでRoCEパケットを送信し、パケットが系列のvport FDBに到達すると、パケットソースvportが一致するルールで不一致が起きる場合があります。

FWバージョン12.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- まれに、署名がされた再送信/パケット損失が原因でエラーが発生し、接続が終了することがあります。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。
- mlxconfigツールが、既存の拡張ROMイメージだけを表示するのでなく、可能なすべての拡張ROMイメージを表示します。
- nic_receive_steering_discard コマンドを実行しているとき、イーサーネットマルチキャストループバックパケットがカウントされません(ローカルループバックパケットでなくても)。
- デュアルポートVHCAが非ネイティブポートでRoCEパケットを送信し、パケットが系列のvport FDBに到達すると、パケットソースvportが一致するルールで不一致が起きる場合があります。
- DC CNAKストレステスト中に、DC CNAKタイムアウト(CNAKドロップ)が発生することがあります。

FWバージョン16.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。

事前要件

HPE Synergy 6410C 25/50Gb Ethernetアダプター(868779-B21)を先に前提となるファームウェアバージョン12.21.2808にアップグレードしてから、12.22.0148または12.22.0194にアップデートする必要があります。
12.22.0194は、HPE Synergy 6410C 25/50Gb Ethernetアダプター(868779-B21)の初のセキュアファームウェアです。いったんこのデバイスをファームウェア12.22.0194にアップグレードすると、ダウングレードができません。

修正

バージョン2.42.5000で提出された修正:

- PortRcvPktsカウンターはリセット後にクリアされませんでした。
- 10個を超える仮想機能がFLRを実行し、完了タイムアウト値が16ミリ秒より小さい範囲に構成されている場合に、VFの構成サイクルでシステムのタイムアウトが発生する問題。
- ドライバーを(別のスレッドから)並行して再起動しているときに、"mlxfwtop –d mt4103_pci_cr0"を実行した場合、サーバーがハングしてNMI(マスク不可能割り込み)になる問題。この場合、デバイスのダウンストリームブリッジは完了タイムアウトエラーを報告しました。
- bmc_rebootの実行後にBMCがIPv6でpingを受信できなかったflow_steeringの問題。
- 存在しないリソースに対してRXパケットが不正なアクセスを引き起こし、その結果QPCGWまたはiriscがスタックする、HCA(ホストチャネルアダプター)を閉じる際の問題。

- ポートがActiveやArmedの状態でない場合に、マスターSMLIDとLIDが0または0xFFFFである問題。
- ibdumpがすべてのMADパケットをキャプチャーできない問題。
- 再起動後にリンクアップしませんでした。
- sw_resetの実行中に到着したPCIeコンフィギュレーションサイクルが2つの完了を生成する原因となる、まれな問題。
- iniファイル内にdisable_stat-ic_steering_iniフィールドを追加したときに、スクラッチパッドでのこのフィールドのメモリ割り当ての問題により、NC-SI(Network Controller Sideband Interface)が動作しなくなる問題。

バージョン14.22.1414 で提出された修正:

- 温度正規化関数の計算問題。純粋整数ではないケーブルゲインの考慮を修正しました。
- 応答で異なる構造の原因になっていたASNのオブジェクト0x8のパーサーに関連する問題を修正しました。
- スタンバイモードでのリブート時にバックプレーンポートケージが意図せず電源オフになることを回避するためのオプションを追加しました。
- LAGが有効な場合にvportの状態をクエリするときに、ドライバーが2つの物理ポートの誤った論理ORを返す原因となる問題を修正しました。
- EDRリンク結果を向上するため、フルワイヤスピード(FWS)しきい値を大きくしました。
- アフィニティQPがオープンの状態でVFがFLRを受信した場合に、"Destroy LAG"コマンドが失敗する問題。
- RoCEデュアルポートモードが有効になっている場合、2番目のポートでtcpdumpが機能しません。

拡張

次のデバイス用のファームウェアが2.42.5000にアップデートされます。

779799-B21 (HP Ethernet 10Gb 2-port 546FLR-SFP+ アダプター)
779793-B21 (HP Ethernet 10Gb 2-port 546SFP+ アダプター)

バージョン2.42.5000の新機能および変更:

- 以下の機能のサポートを追加しました。
  - TLV:CX3_GLOBAL_CONFを使用して、mlxconfig構成を介して着信パケットのタイムスタンプを有効または無効にします。
  - ユーザーMAC構成。
  - ドライバーのリセット前に自動的にmstdumpを収集します。
  - TPT(iron)からDEAD_IRISC(plastic)を検出し、アサートを発生させます。
- コマンドタイムアウトの場合のデバッグ機能を強化しました。
- user_mtuのサイズをファームウェアに示す「set port」 コマンドに新しいコマンドを追加しました。

次のデバイス用のファームウェアが14.22.1414にアップデートされます:

817749-B21 (HPE Ethernet 25Gb 2-port 640FLR-SFP28アダプター)
817753-B21 (HPE Ethernet 25Gb 2-port 640SFP28アダプター)

バージョン14.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **Software Reset Flow:** 致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **Steering Discard Packet Counters:** 廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **仮想機能(VF):** PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで58 VF
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。
- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- **vportミラーリング:** パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性:Special Error Event:** QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。

- QPの作成時間を高速化しました。
- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

次のデバイス用のファームウェアが12.22.1414にアップデートされました:

868779-B21(HPE Synergy 6410C 25/50Gb Ethernetアダプター)

バージョン12.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **Software Reset Flow:** 致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **Steering Discard Packet Counters:** 廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **仮想機能(VF):** PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで58 VF
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。
- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- **vportミラーリング:** パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性:Special Error Event:** QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。
- QPの作成時間を高速化しました。
- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

次のデバイス用のファームウェアが16.22.1414にアップデートされました:

874253-B21(HPE Ethernet 100Gb 1-port 842QSFP28アダプター)

バージョン16.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **Software Reset Flow:** 致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **Steering Discard Packet Counters:** 廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。
- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- Push/Pop VLAN、新しいFLOW TABLE ENTRYアクションのサポートを追加します。これらの新しい操作は、Q-in-Q機能を実装する、ドライバーによって使用されます。
- ConnectX 5 アダプターカードでパケット ペーシングします。
- **vportミラーリング:** パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性:Special Error Event:** QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。
- QPの作成時間を高速化しました。

- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

サポートしているデバイスおよび機能

HPE部品番号	InfiniBandカードタイプ	PSID
779793-B21	HP Ethernet 10Gb 2ポート546SFP+アダプター	HP_1200111023
779799-B21	HP Ethernet 10Gb 2ポート546FLR-SFP+アダプター	HP_2240110004
817749-B21	HPE Ethernet 25Gb 2ポート 640FLR-SFP28 アダプター	HP_2690110034
817753-B21	HPE Ethernet 25Gb 2ポート 640SFP28 アダプター	HP_2420110034
868779-B21	HPE Synergy 6410C 25/50Gb Ethernetアダプター	HPE0000000006
874253-B21	HPE Ethernet 100Gb 1ポート 842QSFP28 アダプター	HPE0000000014

HPE QLogic FastLinQオンラインファームウェアアップグレードユーティリティ for Linux x86_64

バージョン: 1.4.24 **(オプション)**
ファイル名: firmware-nic-qlogic-flq-1.4.24-1.1.x86_64.compsig; firmware-nic-qlogic-flq-1.4.24-1.1.x86_64.rpm

重要な注意！

この製品のファームウェアとともに使用する場合は、*HPE QLogic FastLinQ 10/25/50GbE Drivers for Linux*、バージョン8.33.17.0-1以降を推奨しています。

事前要件

このパッケージには、ご使用のネットワークアダプターのための適切なドライバーがインストールされ、ファームウェアを更新する前にすべてのイーサーネットポートがアップ(*ifup ethX* または*ifconfig ethX up*)している必要があります。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター
- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター

HPE QLogic FastLinQオンラインファームウェアアップグレードユーティリティ for VMware

バージョン: 4.6.24 **(オプション)**
ファイル名: CP033812.compsig; CP033812.zip

重要な注意！

このファームウェアとともに使用する場合は、*HPE QLogic FastLinQ 10/25/50GbE*マルチファンクションドライバー*for VMware*、バージョン2018.06.04以降を推奨しています。

このソフトウェアパッケージは、以下のファームウェアバージョンが含まれています。

NIC	ブートコード(MFW)	UEFIバー	PXEバー	コンボイメージ

	バージョン	ジョン	ジョン	バージョン
HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター	8.35.3.0	4.1.4.25	2.0.17	8.35.09
HPE Synergy 6810C 25/50Gb Ethernetアダプター				
HPE Ethernet 10Gb 2ポート 521Tアダプター	8.35.3.0	4.1.4.25	2.0.17	8.35.09
HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター				
HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター				

事前要件

この製品では、ファームウェアをアップデートする前に、使用するデバイスおよびオペレーティングシステム用の適切なドライバーがインストールされている必要があります。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic FastLinQオンラインファームウェアアップグレードユーティリティ for Windows Server x64 Editions

バージョン: 5.1.3.0 **(オプション)**
ファイル名: cp033845.compsig; cp033845.exe

重要な注意！

この製品のファームウェアとともに使用する場合は、*HPE QLogic FastLinQ 10/25/50GbE*ドライバー*for Windows Server x64 Editions*、バージョン8.33.23.0以降を推奨しています。

事前要件

この製品では、ファームウェアをアップデートする前に、使用するデバイスおよびオペレーティングシステム用の適切なドライバーがインストールされている必要があります。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HPE Ethernet 10Gb 2ポート 521Tアダプター
- HPE Ethernet 4x25Gb 1-port 620QSFP28 アダプター
- HPE Ethernet 10/25Gb 2ポート 621SFP28アダプター
- HPE Ethernet 10/25Gb 2ポート 622FLR-SFP28 コンバージドネットワークアダプター
- HPE Synergy 6810C 25/50Gb Ethernetアダプター

HPE QLogic NX2オンライン ファームウェアアップグレードユーティリティ for VMware

バージョン: 1.22.2 **(オプション)**
ファイル名: CP035389.compsig; CP035389.zip

重要な注意！

このファームウェアとともに使用する場合は、*HPE QLogic NX2 10/20GbE Multifunction Drivers for VMware*、バージョン2018.09.00以降を推奨しています。

このソフトウェアパッケージには、下記のファームウェアバージョンを含むコンボイメージv7.17.19が含まれています:

NIC	ブートコードバージョン	PXEバージョン	UEFIバージョン	iSCSIバージョン	FCoEバージョン	CCMバージョン	L2バージョン
HP Ethernet 10Gb 2ポート 530SFP+アダプター HP Ethernet 10Gb 2ポート 530T ネットワークアダプター	7.15.24	7.14.13	8.2.9	n/a	n/a	7.14.4	7.12.25
HP Ethernet 10Gb 2ポート 533FLR-Tアダプター HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター HP FlexFabric 10Gb 2ポート 534Mアダプター HP FlexFabric 10Gb 2ポート 536FLBアダプター HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター HP FlexFabric 20Gb 2ポート 630FLBアダプター HP FlexFabric 20Gb 2ポート 630Mアダプター HP StoreFabric CN1100R Dual Port Converged Network Adapter HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター HPE Synergy 2820C 10Gbコンバージドネットワークアダプター	7.15.24	7.14.13	8.2.9	7.14.0	7.14.3	7.14.4	7.12.25

事前要件

この製品では、ファームウェアをアップデートする前に、使用するデバイスおよびオペレーティングシステム用の適切なドライバーがインストールされている必要があります。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP Ethernet 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター

- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

HPE QLogic NX2オンラインファームウェアアップグレードユーティリティ for Linux x86_64

バージョン: 2.22.56 **(オプション)**
ファイル名: firmware-nic-qlogic-nx2-2.22.56-1.1.x86_64.compsig; firmware-nic-qlogic-nx2-2.22.56-1.1.x86_64.rpm

重要な注意！

このパッケージのファームウェアとともに使用する場合は、*HPE QLogic NX2 10/20GbE Multifunction Drivers for Linux*、バージョン 7.14.48-2以降を推奨しています。

事前要件

このパッケージには、ご使用のネットワークアダプターのための適切なドライバーがインストールされ、ファームウェアを更新する前にすべてのイーサーネットポートがアップ(*ifup ethX* または*ifconfig ethX up*)している必要があります。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP Ethernet 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター

HPE QLogic NX2オンラインファームウェアアップグレードユーティリティ for Windows Server x64 Edition

バージョン: 5.1.3.0 **(オプション)**
ファイル名: cp034083.compsig; cp034083.exe

重要な注意！

このファームウェアとともに使用する場合は、*HPE QLogic NX2 10/20GbE Multifunction Drivers for Windows Server x64 Edition*、バージョン7.13.145.0以降を推奨しています。

事前要件

この製品では、ファームウェアをアップデートする前に、使用するデバイスおよびオペレーティングシステム用の適切なドライバーがインストールされている必要があります。

修正

この製品は、'System Utilities->System Configuration'メニューのF7キーを押して、アダプターの構成設定をデフォルトに復元しようとすると、エラーメッセージが表示されることがある問題を修正しました。

サポートしているデバイスおよび機能

この製品は、以下のネットワークアダプターをサポートします。

- HP Ethernet 10Gb 2ポート 530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HP Ethernet 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE Synergy 2820C 10Gbコンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

HPEファームウェアフラッシュfor VMware vSphere 6.0用Emulexコンバージドネットワークアダプター

バージョン: 2018.09.01 **(推奨)**
ファイル名: CP035919.compsig; CP035919.zip

重要な注意！

リリースノート:

HPE StoreFabric Emulex アダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

Updated CNA (XE100 series) firmware

ファームウェア

Contains:

CNA (XE100 series) firmware 12.0.1110.10

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HP Ethernet 10Gb 2ポート 557SFP+ アダプター
- HPE StoreFabric CN1200E-Tアダプター

HPEファームウェアフラッシュfor VMware vSphere 6.5用Emulexコンバージドネットワークアダプター

バージョン: 2018.09.01 **(推奨)**
ファイル名: CP035920.compsig; CP035920.zip

重要な注意！

リリースノート:

HPE StoreFabric Emulex アダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

Updated CNA (XE100 series) firmware

ファームウェア

Contains:

CNA (XE100 series) firmware 12.0.1110.10

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HP Ethernet 10Gb 2ポート 557SFP+ アダプター
- HPE StoreFabric CN1200E-Tアダプター

オンラインファームウェアアップグレードユーティリティ (ESXi 6.0) for HPE Mellanox VPI (EthernetおよびInfinibandモード) ConnectX4 devices on VMware ESXi 6.0

バージョン: 1.0.4 **(推奨)**
ファイル名: CP034538.compsig; CP034538.zip

修正

ファームウェアバージョン12.22.4030および 16.22.4030での修正:

- まれに、受信側のエレクトリックアイ幅が狭い場合に、10^-12よりも低いBERでリンクが発生することがあります。
- LROタイムアウト構成が定義済みの静的な値ではなく、TLV構成から取得されるようになりました。
- モジュール温度の読み取りが-40°Cよりも低い場合と125°Cよりも高い場合に無視するフィルターを追加しました。
- Ackがメモリにスキャッターことなく送信するのを防ぐために、高速切断フローの一環としてvportをクローズしました。
- PERST#のアサーション解除が特定の重要な期間に到着した、まれなシナリオが処理されました。
- 温度正規化関数の計算問題。純粋整数ではないケーブルゲインが考慮されるようになりました。
- 応答で異なる構造の原因になっていたASNのオブジェクト0x8の解析。
- HCAがFLRを実行している間、MSIX割り込みが失われた問題が処理されました。
- ファームウェアのブートプロセスとPCIeからのMSIXアクセスの間で競合状態が発生し、これによってMSIXベクトルへの書き込みが失われた問題が修正されました。

拡張

次のデバイス用のファームウェアが12.22.4030にアップデートされました:

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28アダプター)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28アダプター)

バージョン12.22.4030の新機能および変更:

- **AS Notify:** AS Notifyを使用すると、IBMのPower CPUアーキテクチャーでは、軽量な"割り込み"を発行するハードウェアで従来MSI割り込みを置換することにより、パフォーマンスを向上させることができます。
- **Dump Me Now (DMN):** オフラインデバッグするために不可欠なさまざまなコンポーネントからDump Me Now(DMN)で生成したダンプおよびトレース。問題が検出されると、障害時のNICの状態に関する有用な情報をダンプから得られます。
- QP RTS2RTSでのDSCPマッピングのサポートが追加されました。
- **ポートの有効化:** ポートの有効化が設定されると、デバイスは、すべての関連機能に対する"ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters"を使用したリンクダウンのエミュレーションをサポートします。
- **mlxfwreset:** ファームウェアアップデートフローのmlxfwresetロード時間を削減および迅速化しました。
- **仮想機能(VF):** PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで64 VF
- 再試行カウンター(extended_retry_count)の最大値を7ではなく255まで拡張しました。

次のデバイス用のファームウェアが16.22.4030にアップデートされます。

879482-B21 (HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFPアダプター)
872726-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28アダプター)

バージョン16.22.4030の新機能および変更:

- **AS Notify:** AS Notifyを使用すると、IBMのPower CPUアーキテクチャーでは、軽量な"割り込み"を発行するハードウェアで従来MSI割り込みを置換することにより、パフォーマンスを向上させることができます。
- **Dump Me Now (DMN):** オフラインデバッグするために不可欠なさまざまなコンポーネントからDump Me Now(DMN)で生成したダンプおよびトレース。問題が検出されると、障害時のNICの状態に関する有用な情報をダンプから得られます。
- QP RTS2RTSでのDSCPマッピングのサポートが追加されました。
- **ポートの有効化:** ポートの有効化が設定されると、デバイスは、すべての関連機能に対する"ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters"を使用したリンクダウンのエミュレーションをサポートします。
- **mlxfwreset:** ファームウェアアップデートフローのmlxfwresetロード時間を削減および迅速化しました。
- **仮想機能(VF):** PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで64 VF
- 再試行カウンター(extended_retry_count)の最大値を7ではなく255まで拡張しました。
- InfiniBandでRQを拡張するサポートが追加されました。
- **QoS "Rate Limit":** 個々のInfiniBandポートサービスレベルの伝送速度を制限をサポートすることが追加されました。この機能は、新しいベンダー固有MAD(QosConfigSL)を通じて構成できます。

オンラインファームウェアアップグレードユーティリティ (ESXi 6.5) for HPE Mellanox VPI (EthernetおよびInfinibandモード) ConnectX4 devices on VMware ESXi 6.5

バージョン: 1.0.3 **(推奨)**
ファイル名: CP034539.compsig; CP034539.zip

修正

ファームウェアバージョン12.22.4030および 16.22.4030での修正:

- まれに、受信側のエレクトリックアイ幅が狭い場合に、10^-12よりも低いBERでリンクが発生することがあります。
- LROタイムアウト構成が定義済みの静的な値ではなく、TLV構成から取得されるようになりました。
- モジュール温度の読み取りが-40°Cよりも低い場合と125°Cよりも高い場合に無視するフィルターを追加しました。
- Ackがメモリにスキャッターことなく送信するのを防ぐために、高速切断フローの一環としてvportをクローズしました。
- PERST#のアサーション解除が特定の重要な期間に到着した、まれなシナリオが処理されました。
- 温度正規化関数の計算問題。純粋整数ではないケーブルゲインが考慮されるようになりました。
- 応答で異なる構造の原因になっていたASNのオブジェクト0x8の解析。
- HCAがFLRを実行している間、MSIX割り込みが失われた問題が処理されました。
- ファームウェアのブートプロセスとPCIeからのMSIXアクセスの間で競合状態が発生し、これによってMSIXベクトルへの書き込みが失われた問題が修正されました。

拡張

次のデバイス用のファームウェアが12.22.4030にアップデートされました:

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28アダプター)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28アダプター)

バージョン12.22.4030の新機能および変更:

- **AS Notify:** AS Notifyを使用すると、IBMのPower CPUアーキテクチャーでは、軽量な"割り込み"を発行するハードウェアで従来MSI割り込みを置換することにより、パフォーマンスを向上させることができます。
- **Dump Me Now (DMN):** オフラインデバッグするために不可欠なさまざまなコンポーネントからDump Me Now(DMN)で生成したダンプおよびトレース。問題が検出されると、障害時のNICの状態に関する有用な情報をダンプから得られます。
- QP RTS2RTSでのDSCPマッピングのサポートが追加されました。

- **ポートの有効化:** ポートの有効化が設定されると、デバイスは、すべての関連機能に対する"ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters"を使用したリンクダウンのエミュレーションをサポートします。
- **mlxfwreset:** ファームウェアアップデートフローのmlxfwresetロード時間を削減および迅速化しました。
- **仮想機能(VF):** PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで64 VF
- 再試行カウンター(extended_retry_count)の最大値を7ではなく255まで拡張しました。

次のデバイス用のファームウェアが16.22.4030にアップデートされます。

879482-B21 (HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFPアダプター)
872726-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28アダプター)

バージョン16.22.4030の新機能および変更:

- **AS Notify:** AS Notifyを使用すると、IBMのPower CPUアーキテクチャーでは、軽量な"割り込み"を発行するハードウェアで従来MSI割り込みを置換することにより、パフォーマンスを向上させることができます。
- **Dump Me Now (DMN):** オフラインデバッグするために不可欠なさまざまなコンポーネントからDump Me Now(DMN)で生成したダンプおよびトレース。問題が検出されると、障害時のNICの状態に関する有用な情報をダンプから得られます。
- QP RTS2RTSでのDSCPマッピングのサポートが追加されました。
- **ポートの有効化:** ポートの有効化が設定されると、デバイスは、すべての関連機能に対する"ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters"を使用したリンクダウンのエミュレーションをサポートします。
- **mlxfwreset:** ファームウェアアップデートフローのmlxfwresetロード時間を削減および迅速化しました。
- **仮想機能(VF):** PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで64 VF
- 再試行カウンター(extended_retry_count)の最大値を7ではなく255まで拡張しました。
- InfiniBandでRQを拡張するサポートが追加されました。
- **QoS "Rate Limit":** 個々のInfiniBandポートサービスレベルの伝送速度を制限をサポートすることが追加されました。この機能は、新しいベンダー固有MAD(QosConfigSL)を通じて構成できます。

オンラインファームウェアアップグレードユーティリティ (Linux x86_64) for HPE Intel OPA adapters

バージョン: 1.6.0 (A) **(推奨)**
ファイル名: 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

修正

バージョン1.6.0(A)での修正:

1. デフォルトの最初のアダプターだけではなく、選択したすべてのOPA HFIアダプターのTMMをアップデートします
2. 重複したCP.xmlおよびpayload.jsonファイルを削除しました。

オンラインファームウェアアップグレードユーティリティ (Linux x86_64) for HPE Mellanox IB only ConnectX4 device on Linux x86_64 platform

バージョン: 1.0.2 **(推奨)**
ファイル名: 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

修正

ファームウェアバージョン12.22.4030および 16.22.4030での修正:

- まれに、受信側のエレクトリックアイ幅が狭い場合に、10^-12よりも低いBERでリンクが発生することがあります。
- LROタイムアウト構成が定義済みの静的な値ではなく、TLV構成から取得されるようになりました。
- モジュール温度の読み取りが-40°Cよりも低い場合と125°Cよりも高い場合に無視するフィルターを追加しました。

- Ackがメモリにスキャッターことなく送信するのを防ぐために、高速切断フローの一環としてvportをクローズしました。
- PERST#のアサーション解除が特定の重要な期間に到着した、まれなシナリオが処理されました。
- 温度正規化関数の計算問題。純粋整数ではないケーブルゲインが考慮されるようになりました。
- 応答で異なる構造の原因になっていたASNのオブジェクト0x8の解析。
- HCAがFLRを実行している間、MSIX割り込みが失われた問題が処理されました。
- ファームウェアのブートプロセスとPCIeからのMSIXアクセスの間で競合状態が発生し、これによってMSIXベクトルへの書き込みが失われた問題が修正されました。

拡張

次のデバイス用のファームウェアが12.22.4030にアップデートされました:

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28アダプター)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28アダプター)

バージョン12.22.4030の新機能および変更:

- **AS Notify:** AS Notifyを使用すると、IBMのPower CPUアーキテクチャーでは、軽量な"割り込み"を発行するハードウェアで従来MSI割り込みを置換することにより、パフォーマンスを向上させることができます。
- **Dump Me Now (DMN):** オフラインデバッグするために不可欠なさまざまなコンポーネントからDump Me Now(DMN)で生成したダンプおよびトレース。問題が検出されると、障害時のNICの状態に関する有用な情報をダンプから得られます
- QP RTS2RTSでのDSCPマッピングのサポートが追加されました。
- **ポートの有効化:** ポートの有効化が設定されると、デバイスは、すべての関連機能に対する"ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters"を使用したリンクダウンのエミュレーションをサポートします。
- **mlxfwreset:** ファームウェアアップデートフローのmlxfwresetロード時間を削減および迅速化しました。
- **仮想機能 (VF):** PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで64 VF
- 再試行カウンター(extended_retry_count)の最大値を7ではなく255まで拡張しました。

次のデバイス用のファームウェアが16.22.4030にアップデートされます。

879482-B21 (HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFPアダプター)
872726-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28アダプター)

バージョン16.22.4030の新機能および変更:

- **AS Notify:** AS Notifyを使用すると、IBMのPower CPUアーキテクチャーでは、軽量な"割り込み"を発行するハードウェアで従来MSI割り込みを置換することにより、パフォーマンスを向上させることができます。
- **Dump Me Now (DMN):** オフラインデバッグするために不可欠なさまざまなコンポーネントからDump Me Now(DMN)で生成したダンプおよびトレース。問題が検出されると、障害時のNICの状態に関する有用な情報をダンプから得られます
- QP RTS2RTSでのDSCPマッピングのサポートが追加されました。
- **ポートの有効化:** ポートの有効化が設定されると、デバイスは、すべての関連機能に対する"ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters"を使用したリンクダウンのエミュレーションをサポートします。
- **mlxfwreset:** ファームウェアアップデートフローのmlxfwresetロード時間を削減および迅速化しました。
- **仮想機能 (VF):** PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで64 VF
- 再試行カウンター(extended_retry_count)の最大値を7ではなく255まで拡張しました。
- InfiniBandでRQを拡張するサポートが追加されました。
- **QoS "Rate Limit":** 個々のInfiniBandポートサービスレベルの伝送速度を制限をサポートすることが追加されました。この機能は、新しいベンダー固有MAD(QosConfigSL)を通じて構成できます。

オンラインファームウェアアップグレードユーティリティ (Linux x86_64) for HPE Mellanox VPI (EthernetおよびInfinibandモード) ConnectX4 devices on Linux x86_64 platform

バージョン: 1.0.4 **(推奨)**
ファイル名: 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

修正

ファームウェアバージョン12.22.4030および 16.22.4030での修正:

- まれに、受信側のエレクトリックアイ幅が狭い場合に、10^-12よりも低いBERでリンクが発生することがあります。
- LROタイムアウト構成が定義済みの静的な値ではなく、TLV構成から取得されるようになりました。
- モジュール温度の読み取りが-40°Cよりも低い場合と125°Cよりも高い場合に無視するフィルターを追加しました。
- Ackがメモリにスキャッターことなく送信するのを防ぐために、高速切断フローの一環としてvportをクローズしました。
- PERST#のアサーション解除が特定の重要な期間に到着した、まれなシナリオが処理されました。
- 温度正規化関数の計算問題。純粋整数ではないケーブルゲインが考慮されるようになりました。
- 応答で異なる構造の原因になっていたASNのオブジェクト0x8の解析。
- HCAがFLRを実行している間、MSIX割り込みが失われた問題が処理されました。
- ファームウェアのブートプロセスとPCIeからのMSIXアクセスの間で競合状態が発生し、これによってMSIXベクトルへの書き込みが失われた問題が修正されました。

拡張

次のデバイス用のファームウェアが12.22.4030にアップデートされました:

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28アダプター)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28アダプター)

バージョン12.22.4030の新機能および変更:

- **AS Notify:** AS Notifyを使用すると、IBMのPower CPUアーキテクチャーでは、軽量な"割り込み"を発行するハードウェアで従来MSI割り込みを置換することにより、パフォーマンスを向上させることができます。
- **Dump Me Now (DMN):** オフラインデバッグするために不可欠なさまざまなコンポーネントからDump Me Now(DMN)で生成したダンプおよびトレース。問題が検出されると、障害時のNICの状態に関する有用な情報をダンプから得られます。
- QP RTS2RTSでのDSCPマッピングのサポートが追加されました。
- **ポートの有効化:** ポートの有効化が設定されると、デバイスは、すべての関連機能に対する"ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters"を使用したリンクダウンのエミュレーションをサポートします。
- **mlxfwreset:** ファームウェアアップデートフローのmlxfwresetロード時間を削減および迅速化しました。
- **仮想機能(VF):** PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで64 VF
- 再試行カウンター(extended_retry_count)の最大値を7ではなく255まで拡張しました。

次のデバイス用のファームウェアが16.22.4030にアップデートされます。

879482-B21 (HPE InfiniBand FDR/Ethernet 40/50Gb 2-port 547FLR-QSFPアダプター)
872726-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 841QSFP28アダプター)

バージョン16.22.4030の新機能および変更:

- **AS Notify:** AS Notifyを使用すると、IBMのPower CPUアーキテクチャーでは、軽量な"割り込み"を発行するハードウェアで従来MSI割り込みを置換することにより、パフォーマンスを向上させることができます。
- **Dump Me Now (DMN):** オフラインデバッグするために不可欠なさまざまなコンポーネントからDump Me Now(DMN)で生成したダンプおよびトレース。問題が検出されると、障害時のNICの状態に関する有用な情報をダンプから得られます。
- QP RTS2RTSでのDSCPマッピングのサポートが追加されました。

- **ポートの有効化:** ポートの有効化が設定されると、デバイスは、すべての関連機能に対する"ICMD_SET_VIRTUAL_PARAMETERS - Set Device Virtual Parameters"を使用したリンクダウンのエミュレーションをサポートします。
- **mlxfwreset:** ファームウェアアップデートフローのmlxfwresetロード時間を削減および迅速化しました。
- **仮想機能(VF):** PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで64 VF
- 再試行カウンター(extended_retry_count)の最大値を7ではなく255まで拡張しました。
- InfiniBandでRQを拡張するサポートが追加されました。
- **QoS "Rate Limit":** 個々のInfiniBandポートサービスレベルの伝送速度を制限をサポートすることが追加されました。この機能は、新しいベンダー固有MAD(QosConfigSL)を通じて構成できます。

オンラインファームウェアアップグレードユーティリティ (Windows x64) for HPE Mellanox IB only ConnectX4 device on Windows x86_64 platform

バージョン: 1.0.0.2 (A) **(推奨)**
ファイル名: cp037169.compsig; cp037169.exe

修正

バージョン12.14.1100での修正:

- RDMA_CMドライバーがキューペア(QP)レートの制限を予期せずにアクティブにしたことで、このQPが帯域幅が大幅に減少していました。
- 明示的な輻輳通知(ECN)を多対一のシナリオでは有効にすると、スループットが低くなります。
- ファームウェアをハングアップさせたまれな問題です。
- セットアップでの最高温度は、実温度に関係なく現在の温度として報告されます。
- 仮想アドレス機能 NC-SI (サイドバンド) での誤ったレポート。
- Vcoreあたりの拡張された受信感度。
- モジュールの初期化時に NACK の受信を避けるために保護されたモジュールに記述するオプションを無効にします。
- すべてのECを無効にするinvalidate_allコマンドを送信すると、cold_flicksがリセットされます。
- SR-IOV最小および最大レートリミッターは、ポートごとに最大64個の仮想関数(VF)のみをサポートできます。
- 明示的輻輳通知(ECN)は、ホストあたり～500個のQPの数のときには、予想どおりに機能しませんでした。
- SR-IOV上のUnreliable Datagram(UD)RDMA over Converged Ethernet(RoCE)マルチキャストトラフィックを使用すると、e-se FDB内の指定されたvportだけでなく、e-sw(PFおよびそのVF)内のすべての接続QPにパケットが散在していました。

拡張

次のデバイス用のファームウェアが12.21.1000にアップデートされました:

843400-B21 (HPE Apollo A10 InfiniBand EDR (100Gb) 2-port アダプター)

バージョン12.21.1000の新機能および変更:

- 以下の機能のサポートを追加しました。
  - InfiniBandネイティブ(非SR-IOV)デュアルポートデバイス(ポートごとの機能は無効)。このモードでは、仮想化はサポートされず、ISSI = 0になります。
  - 100GbE AOC /トランシーバーとMellanox以外のデバイスの10G / 40G。
- PTP パケットのタイムスタンプは、ポートにパケットの到着時に有効です。
- 明示的輻輳通知 (ECN) は、イーサネット ポート上のすべてのプロパティに対して既定で有効です。
- DC CNAKは送信されたCNAKのパフォーマンスを向上させ、ConnectX-4アダプターカードの後方圧力を回避します。
- 受信信号の整合性の向上。
  - 信号の整合性を向上させるために、15チックを超える位相でのみリンクを発生させます。
  - 2つの類似した RX 構成間の拡張測定テスト。
  - 2番目の入力バッファーを使用して、信号の整合性を向上させるデータ パスに移動します。
- RDMA Over Converged Ethernet(RoCE)デュアルポートモードでは、デュアルポートVirtual HCA(vHCA)を使用して2つのEthernet(RoCE)NICネットワークポート間でRDMAリソース(MR、CQ、SRQ、PDなど)の使用を有効にし、デュア

ルポートデバイスとしてのNICを表示します。この機能が正しく機能するためには、次の要件を満たす必要があります。
    - LAGまたはデュアル ポート モードは、ドライバーによって有効になっています。
    - デュアル ポート デバイス: 両方のポートをETHとして設定する必要があります。
    - ConnectX-4 / ConnectX-4 Lxアダプターカードでは、1 PFあたりの最大VF数は32です。
    - ポートごとの機能を有効にします。
- DSCPおよび優先度の間の動的マッピングをサポートするために、QPDPMレジスタが追加されました。
- DSCPまたはPCPに応じたQoS優先順位付けの信頼レベルを追加しました。
- 入力バッファー管理が次の目的で追加されました。
    - 優先順位に応じた入力トラフィックのバッファーとのマッピング
    - バッファーサイズとロスレスパラメーター
- 強化されたステアリングルールは、1秒あたり最大50Kのルールにレートを更新します。
- Windows-over-Windowsセットアップのための Windowsシングルルート入出力仮想化(SR-IOV)拡張eIPoIB(セキュア接続なし)を有効にしました。
- crdump操作は、デバイスのcrspace dword-by-dwordのスナップショットをとります。 これにより、ドライバーはファームウェアの障害発生時にデバッグ情報を収集することができます。
- Secure Firmware Updatesによりデバイスは新しいファームウェアバイナリのデジタル署名を検証できるため、正式に認可されたバージョンだけをデバイスにインストールできるようになります。
- Reed Solomon(RS)からFCに減衰16以下のケーブルのデフォルトのForward Error Connection(FEC)モードを変更しました。

オンラインファームウェアアップグレードユーティリティ (Windows x64) for HPE Mellanox VPI (EthernetおよびInfinibandモード) ConnectX4 devices on Windows x86_64 platform

バージョン: 1.0.0.4 (A) **(推奨)**
ファイル名: cp037170.compsig; cp037170.exe

修正

バージョン12.14.1100での修正:

- RDMA_CMドライバーがキューペア(QP)レートの制限を予期せずにアクティブにしたことで、このQPが帯域幅が大幅に減少していました。
- 明示的な輻輳通知(ECN)を多対一のシナリオでは有効にすると、スループットが低くなります。
- ファームウェアをハングアップさせたまれな問題です。
- セットアップでの最高温度は、実温度に関係なく現在の温度として報告されます。
- 仮想アドレス機能 NC-SI (サイドバンド) での誤ったレポート。
- Vcoreあたりの拡張された受信感度。
- モジュールの初期化時に NACK の受信を避けるために保護されたモジュールに記述するオプションを無効にします。
- すべてのECを無効にするinvalidate_allコマンドを送信すると、cold_flicksがリセットされます。
- SR-IOVの最小および最大レートリミッターは、ポートごとに最大64のVFしかサポートできません。
- 明示的輻輳通知(ECN)は、ホストあたり～500個のキューのペア(QP)の数のときには、予想どおりに機能しませんでした。
- SR-IOV上のUnreliable Datagram(UD)RDMA over Converged Ethernet(RoCE)マルチキャストトラフィックを使用すると、e-se FDB内の指定されたvportだけでなく、e-sw(PFおよびそのVF)内のすべての接続QPにパケットが散在していました。

拡張

次のデバイス用のファームウェアが12.21.1000にアップデートされました:

825110-B21 (HPE InfiniBand EDR/Ethernet 100Gb 1-port 840QSFP28アダプター)
825111-B21 (HPE InfiniBand EDR/Ethernet 100Gb 2-port 840QSFP28アダプター)

バージョン12.21.1000の新機能および変更:

- 以下の機能のサポートを追加しました。
    - InfiniBandネイティブ(非SR-IOV)デュアルポートデバイス(ポートごとの機能は無効)。このモードでは、仮想化はサポートされず、ISSI = 0になります。

        - 100GbE AOC /トランシーバーとMellanox以外のデバイスの10G / 40G。
    - PTP パケットのタイムスタンプは、ポートにパケットの到着時に有効です。
    - 明示的輻輳通知 (ECN) は、イーサネット ポート上のすべてのプロパティに対して既定で有効です。
    - DC CNAKは送信されたCNAKのパフォーマンスを向上させ、ConnectX-4アダプターカードの後方圧力を回避します。
    - 受信信号の整合性の向上。
        - 信号の整合性を向上させるために、15チックを超える位相でのみリンクを発生させます。
        - 2 つの類似した RX 構成間の拡張測定テスト。
        - 2番目の入力バッファーを使用して、信号の整合性を向上させるデータ パスに移動します。
    - RDMA Over Converged Ethernet(RoCE)デュアルポートモードでは、デュアルポートVirtual HCA(vHCA)を使用して2つのEthernet(RoCE)NICネットワークポート間でRDMAリソース(MR、CQ、SRQ、PDなど)の使用を有効にし、デュアルポートデバイスとしてのNICを表示します。この機能が正しく機能するためには、次の要件を満たす必要があります。
        - LAGまたはデュアル ポート モードは、ドライバーによって有効になっています。
        - デュアル ポート デバイス: 両方のポートをETHとして設定する必要があります。
        - ConnectX-4 / ConnectX-4 Lxアダプターカードでは、1 PFあたりの最大VF数は32です。
        - ポートごとの機能を有効にします。
    - DSCPおよび優先度の間の動的マッピングをサポートするために、QPDPMレジスタが追加されました。
    - DSCPまたはPCPに応じたQoS優先順位付けの信頼レベルを追加しました。
    - 入力バッファ管理が次の目的で追加されました。
        - 優先順位に応じた入力トラフィックのバッファーとのマッピング
        - バッファーサイズとロスレスパラメーター
    - 強化されたステアリングルールは、1秒あたり最大50Kのルールにレートを更新します。
    - Windows-over-Windowsセットアップのための Windowsシングルルート入出力仮想化(SR-IOV)拡張eIPoIB(セキュア接続なし)を有効にしました。
    - crdump操作は、デバイスのcrspace dword-by-dwordのスナップショットをとります。 これにより、ドライバーはファームウェアの障害発生時にデバッグ情報を収集することができます。
    - Secure Firmware Updatesによりデバイスは新しいファームウェアバイナリのデジタル署名を検証できるため、正式に認可されたバージョンだけをデバイスにインストールできるようになります。
    - Reed Solomon(RS)からFCに減衰16以下のケーブルのデフォルトのForward Error Connection(FEC)モードを変更しました。

オンラインファームウェアアップグレードユーティリティ (ESXi 6.0) for HPE Mellanox VPI (EthernetおよびInfinibandモード)デバイス - VMware ESXi 6.0

バージョン: 1.0.6 **(推奨)**
ファイル名: CP033386.compsig; CP033386.zip

修正

バージョン2.40.5030および2.40.5072での修正:

- ドライバーの起動中にファームウェアとハードウェアの競合が発生し、送信の完了がブロックされました。
- そのファームウェアはclose_portコマンドを実行している間、ドライバーにlink_downイベントを送りませんでした。

バージョン2.42.5000での修正:

- PortRcvPktsカウンターはリセット後にクリアされませんでした。
- 10個を超える仮想機能がFLRを実行し、完了タイムアウト値が16ミリ秒より小さい範囲に構成されている場合に、仮想機能(VF)の構成サイクルでシステムのタイムアウトが発生する問題。
- ドライバーを(別のスレッドから)並行して再起動しているときに、"mlxfwtop –d mt4103_pci_cr0"を実行した場合、サーバーがハングしてNMIになります。この場合、デバイスのダウンストリームブリッジは完了タイムアウトエラーを報告しました。
- bmc_rebootの実行後にBMCがIPv6でpingを受信できなかったflow_steeringの問題。
- HCAを閉じている間、RXパケットは存在しなかったリソースへの不正アクセスを引き起こし、その結果QPCGWまたはiriscがスタックしました。
- ポートがActiveやArmedの状態でない場合に、マスターSMLIDとLIDが0または0xFFFFである問題。
- ibdumpがすべてのMADパケットをキャプチャーできない問題。
- 再起動後にリンクアップしませんでした。

- sw_resetの実行中に到着したPCIeコンフィギュレーションサイクルが2つの完了を生成する原因となる、まれな問題を修正しました。
- iniファイル内にdisable_stat-ic_steering_iniフィールドを追加したときに、スクラッチパッドでのこのフィールドのメモリ割り当ての問題により、ネットワークコントローラー サイドバンドインターフェイス(NC-SI)が動作しなくなる問題。

バージョン2.42.5004での修正:

- UEFI(Unified Extensible Firmware Interface)HII(ヒューマンインターフェイスインフラストラクチャ)メニューでは、HPE Gen10デバイスを使用すると、両方のポートがポート1として表示されます。
- UEFI(Unified Extensible Firmware Interface)のブートメニューで、HPE Gen10デバイスを使用すると、デバイス名に不要なポート番号が表示されます。

拡張

次のデバイス用のファームウェアが2.40.5030にアップデートされました。
764286-B21
778509-B21

次のデバイス用のファームウェアが2.40.5072にアップデートされました。
764285-B21

次のデバイス用のファームウェアが2.42.5004にアップデートされます。
764283-B21
764284-B21

次のデバイス用のファームウェアが2.42.5000にアップデートされます。
764282-B21

ファームウェアバージョン2.40.5030での新機能:

- 以下の機能のサポートを追加しました。
  - MADセンシングやNCSI/IPMI OEMコマンドに関する温度しきい値の高/低デフォルト。
  - user_mtuのサイズをファームウェアに示す"set port"コマンドに新しいフィールドの追加。
  - ファームウェアが内部QPで受信されたパケットを落としたり、WQEプロデューサーフェッチングを使用不可にすることを確認する保護メカニズム。

ファームウェアバージョン2.40.5072での新機能:

- Platform Level Data Model(PLDM)のサポート。

ファームウェアバージョン2.42.5000での新機能:

- 以下の機能のサポートを追加しました。
  - 新しいTLV:CX3_GLOBAL_CONFを使用して、mlxconfig構成を介して着信パケットのタイムスタンプを有効または無効にします。
  - ユーザーMAC構成。
  - ドライバーのリセット前に自動的にmstdumpを収集します。
  - TPT(iron)からDEAD_IRISC(plastic)を検出し、アサートを発生させるメカニズム。
  - user_mtuのサイズをファームウェアに示す"set port"コマンドに新しいフィールドの追加。
- コマンドタイムアウトの場合のデバッグ機能が向上しました。

オンラインファームウェアアップグレードユーティリティ (ESXi 6.5) for HPE Mellanox VPI (EthernetおよびInfinibandモード) デバイス - VMware ESXi 6.5

バージョン: 1.0.1 **(推奨)**
ファイル名: CP033387.compsig; CP033387.zip

修正

バージョン2.40.5030および2.40.5072での修正:

- ドライバーの起動中にファームウェアとハードウェアの競合が発生し、送信の完了がブロックされました。
- そのファームウェアはclose_portコマンドを実行している間、ドライバーにlink_downイベントを送りませんでした。

バージョン2.42.5000での修正:

- PortRcvPktsカウンターはリセット後にクリアされませんでした。
- 10個を超える仮想機能がFLRを実行し、完了タイムアウト値が16ミリ秒より小さい範囲に構成されている場合に、仮想機能(VF)の構成サイクルでシステムのタイムアウトが発生する問題。
- ドライバーを(別のスレッドから)並行して再起動しているときに、"mlxfwtop –d mt4103_pci_cr0"を実行した場合、サーバーがハングしてNMIになります。この場合、デバイスのダウンストリームブリッジは完了タイムアウトエラーを報告しました。
- bmc_rebootの実行後にBMCがIPv6でpingを受信できなかったflow_steeringの問題。
- HCAを閉じている間、RXパケットは存在しなかったリソースへの不正アクセスを引き起こし、その結果QPCGWまたはiriscがスタックしました。
- ポートがActiveやArmedの状態でない場合に、マスターSMLIDとLIDが0または0xFFFFである問題。
- ibdumpがすべてのMADパケットをキャプチャーできない問題。
- 再起動後にリンクアップしませんでした。
- sw_resetの実行中に到着したPCIeコンフィギュレーションサイクルが2つの完了を生成する原因となる、まれな問題を修正しました。
- iniファイル内にdisable_stat-ic_steering_iniフィールドを追加したときに、スクラッチパッドでのこのフィールドのメモリ割り当ての問題により、ネットワークコントローラー サイドバンドインターフェイス(NC-SI)が動作しなくなる問題。

バージョン2.42.5004での修正:

- UEFI(Unified Extensible Firmware Interface)HII(ヒューマンインターフェイスインフラストラクチャ)メニューでは、HPE Gen10デバイスを使用すると、両方のポートがポート1として表示されます。
- UEFI(Unified Extensible Firmware Interface)のブートメニューで、HPE Gen10デバイスを使用すると、デバイス名に不要なポート番号が表示されます。

拡張

次のデバイス用のファームウェアが2.40.5030にアップデートされました。
764286-B21
778509-B21

次のデバイス用のファームウェアが2.40.5072にアップデートされました。
764285-B21

次のデバイス用のファームウェアが2.42.5004にアップデートされます。
764283-B21
764284-B21

次のデバイス用のファームウェアが2.42.5000にアップデートされます。
764282-B21

ファームウェアバージョン2.40.5030での新機能:

- 以下の機能のサポートを追加しました。
  - MADセンシングやNCSI/IPMI OEMコマンドに関する温度しきい値の高/低デフォルト。
  - user_mtuのサイズをファームウェアに示す"set port"コマンドに新しいフィールドの追加。
  - ファームウェアが内部QPで受信されたパケットを落としたり、WQEプロヂューサーフェッチングを使用不可にすることを確認する保護メカニズム。

ファームウェアバージョン2.40.5072での新機能:

- Platform Level Data Model(PLDM)のサポート。

ファームウェアバージョン2.42.5000での新機能:

- 以下の機能のサポートを追加しました。
  - 新しいTLV:CX3_GLOBAL_CONFを使用して、mlxconfig構成を介して着信パケットのタイムスタンプを有効または無効にします。

        - ユーザーMAC構成。
        - ドライバーのリセット前に自動的にmstdumpを収集します。
        - TPT(iron)からDEAD_IRISC(plastic)を検出し、アサートを発生させるメカニズム。
        - user_mtuのサイズをファームウェアに示す"set port"コマンドに新しいフィールドの追加。
    - コマンドタイムアウトの場合のデバッグ機能が向上しました。

オンラインファームウェアアップグレードユーティリティ (Linux x86_64) for HPE Infiniband FDR 2P 545QSFPアダプター (HP部品番号702211-B21)、 HPE Infiniband FDR 2P 545FLR-QSFP アダプター (HP部品番号702212-B21) および HPE Infiniband FDR 2P 545M アダプター(HP部品番号702213-B21)

バージョン: 1.0.6 **(推奨)**
ファイル名: 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

修正

ファームウェアバージョン10.16.1058で、以下の問題を解決しました。:

- SR-IOVを有効にするとシステムのエラーとなる問題を修正しました。
- SRQ制限イベントがトリガーされるとRXがハングするまれな問題を修正しました。
- WQEフェッチにおけるPCIエラーを受信した時DCにおいてRXトラフィックがしばしば停止する原因に関する問題点を修正しました。
- VF_LOG_BAR_SIZEのmlxconfig構成が無視され、5(32MB)に設定される問題を修正しました。
- ファームウエアがハングする原因となるPCIからのEEHエラーを修正しました。
- VLウエイト 0でSMを構成し、その上でトラフィックを実行しているときに、一部のVLでアンロード中にドライバーが時折ハングする原因となる問題を修正しました。
- 再送信が起こりRXが同じパケットを2回受け取るとういケースでDCトランスポートが有効の場合に、アサートがドライバーにレポートされる原因となったまれなケースを修正しました
- VFのGUID構成がステアリングテーブルで過負荷のときにVFのvportを有効化/無効化すると、HCAがハングする原因となる問題を修正しました。

ファームウェアバージョン10.16.1038で、以下の問題を解決しました。:

- RSODバグを修正しました。
- 物理ポートTLVをポート2に問い合わせおよび書き込むためにシングルポートデバイスに生じる問題を解決しました。
- qkey/pkey違反カウンターをport_info mad経由でリセットしている場合に、デバイスのハングを引き起こす問題が修正されました。
- パケットの喪失シナリオ下のRDMA READ帯域幅が改善されました。
- PFドライバーまたはツール (例えば、ethtool) がPAOS DOWNコマンド (例えば、ifconfig downまたはip link set down) を使用している場合、ループバックトラフィックは、このポート (PF<->VFs / VF<->VF) 上のすべての機能をブロックします。
  マルチホスト ループバックでは、このトラフィックは、ファームウェアがすべてのPFからPAOS downコマンドを受け取ると、ブロックされます。しかし、ループバックトラフィックは、物理リンクが原因でダウンする場合にはブロックされません(例えば:ケーブルのプラグ外れ、スイッチポートがダウン)。
- memopマシンへ渡されるリザーブlkeyのQP許可を妨げた問題を修正しました。
- WQEのSLがQPのSLと異なっていた際に発生したMLX QP SLの不一致の処理を修正しました。
- 誤ったSM SL2VL構成の実装を修正しました。
- いくつかのケースで不適切な完了が送信されたDC再接続フローを修正しました。
- DCI SQからDCR SQを分離することでDCのパフォーマンス問題を修正しました。
- ibdiagnetを実行するときにファームウェアのハングを引き起こす問題を修正しました。受信されたDiagData MADには以下の数値が含まれていました。
  • Clear_all = 1
  • PageNum = 0
  • Port_select = 0
  ファームウェアがハングしないようにするためには、ポートチェックをSet()に追加しました。
- ibdumpを実行する時のハードウエアの致命的エラーの原因となる問題点を修正しました。
- ハードウェア速度からPRM速度への2度の変換機能の使用により、誤ったFDR10速度表示が報告された問題を修正しました。

- ポートの次の状態が無効だった時の物理マネージャーPCSイベント処理を修正しました。
- EyeOpening MADにより返された不正なデータの原因となる問題点を解決しました。
- VFに関するVF ICMフットプリントを削減しました。
- 正規のメモリ領域の数を2^21から2^22へ増やしました。
- 連続する接続パケットの不適切な扱いを修正しました。
- まれなケースにおいて、PXEのブートの後にポートの速度はより速い速度の代わりにSDRとして到着しました。
- 非常にまれなケースにおいて、ファームウエアはボードの温度超過警告を誤って報告しました。
- DCT ポートがダウンしている間に、destroy-DCTコマンド操作は遅延を経験する場合があります。
- 診断カウンターがVS-MADパージを誤ったアドレスでスタートするようにオフセットさせるという問題を解決しました。
- no-local-DC-resourcesのイベントにおいて安定性上の問題を解決しました。
- 複数のDCTエラーの不適切な操作の問題を解決しました。
- DC RNR の状態の悪い操作の問題を解決しました。
- DCTのdestroy firmware handling timeを削減しました。
- LLRがアクティブの時に起こったリンクフラップの問題を解決しました。
- 廃止されたコード0x0c0600は0x020700に変更されました (InfiniBandネットワークアダプター)。
- アトミックの応答エンディアンは常にビッグなエンディアンです。
- **[PRM v2.01のドキュメント修正、ファームウェアコードの修正はなし。]**
  ポート非同期イベントのドキュメントはPRMとは異なります。全てのポートのイベントは0x9というタイプ値を持っています。
  次のサブタイプ値が下記のイベントで使用されています。
  - 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)は、パスの移行に失敗した場合、1つの関連する非同期エラーイベントだけを起こします。
- 信頼性の高い接続 (RC) QPを作成するときに、0x5のmin_rnr_nak値を使用すると、障害の原因となります。
- まれに、DC Initiator完了が失われる可能性があります。
- 次の署名ルールはサポートされていません。 (PRMでの「署名ルールテーブル」に基づく番号付け)
  - Rule #12: T10 DIF
  - Rule #13: T10 DIF CS
  - Rule #14 T10 DIF CS
- VLアービトレーション構成はVLとして構成された最小帯域幅を保証しませんでした。
- ごくまれに、誤ったファームウェア「hanged(停止)」レポートがdmesgに出力されました。
- CQバッファーサイズ変更がサポートされていません。
- InfiniScaleファミリースイッチおよび非Mellanox InfiniBandスイッチへ接続する場合、DDRおよびQDR速度が回線エラーを報告することがあり、場合によってはSDR速度にダウングレードすることがあります。

拡張

次のデバイス対応ファームウェアが10.16.1038にアップデートされます:

702211-B21 (HP Infiniband FDR 2P 545QSFPアダプター)
702212-B21 (HP Infiniband FDR 2P 545FLR-QSFPアダプター)

次のデバイス対応ファームウェアが10.16.1058にアップデートされます:

702213-B21 (HP Infiniband FDR 2P 545Mアダプター)

ファームウェアバージョン10.16.1038での新機能:

- PFごとのVFの数を32から64に増やしました。
  注:VF数の増加では、以下の制限を考慮する必要があります。
  - 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)
- VPD読み取り専用タグにv1、v3、v6タグを追加しました。

オンラインファームウェアアップグレードユーティリティ (Linux x86_64) for HPE Mellanox VPI (EthernetおよびInfinibandモード)デバイス - Linux x86_64プラットフォーム

バージョン: 1.0.6 **(推奨)**
ファイル名: 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

修正

バージョン2.40.5030および2.40.5072での修正:

- ドライバーの起動中にファームウェアとハードウェアの競合が発生し、送信の完了がブロックされました。
- そのファームウェアはclose_portコマンドを実行している間、ドライバーにlink_downイベントを送りませんでした。

バージョン2.42.5000での修正:

- PortRcvPktsカウンターはリセット後にクリアされませんでした。
- 10個を超える仮想機能がFLRを実行し、完了タイムアウト値が16ミリ秒より小さい範囲に構成されている場合に、仮想機能(VF)の構成サイクルでシステムのタイムアウトが発生する問題。
- ドライバーを(別のスレッドから)並行して再起動しているときに、"mlxfwtop –d mt4103_pci_cr0"を実行した場合、サーバーがハングしてNMIになります。この場合、デバイスのダウンストリームブリッジは完了タイムアウトエラーを報告しました。
- bmc_rebootの実行後にBMCがIPv6でpingを受信できなかったflow_steeringの問題。
- HCAを閉じている間、RXパケットは存在しなかったリソースへの不正アクセスを引き起こし、その結果QPCGWまたはiriscがスタックしました。
- ポートがActiveやArmedの状態でない場合に、マスターSMLIDとLIDが0または0xFFFFである問題。
- ibdumpがすべてのMADパケットをキャプチャーできない問題。
- 再起動後にリンクアップしませんでした。
- sw_resetの実行中に到着したPCIeコンフィギュレーションサイクルが2つの完了を生成する原因となる、まれな問題を修正しました。
- iniファイル内にdisable_stat-ic_steering_iniフィールドを追加したときに、スクラッチパッドでのこのフィールドのメモリ割り当ての問題により、ネットワークコントローラー サイドバンドインターフェイス(NC-SI)が動作しなくなる問題。

バージョン2.42.5004での修正:

- UEFI(Unified Extensible Firmware Interface)HII(ヒューマンインターフェイスインフラストラクチャ)メニューでは、HPE Gen10デバイスを使用すると、両方のポートがポート1として表示されます。
- UEFI(Unified Extensible Firmware Interface)のブートメニューで、HPE Gen10デバイスを使用すると、デバイス名に不要なポート番号が表示されます。

拡張

次のデバイス用のファームウェアが2.40.5030にアップデートされました。
764286-B21
778509-B21

次のデバイス用のファームウェアが2.40.5072にアップデートされました。
764285-B21

次のデバイス用のファームウェアが2.42.5004にアップデートされます。
764283-B21
764284-B21

次のデバイス用のファームウェアが2.42.5000にアップデートされます。
764282-B21

ファームウェアバージョン2.40.5030での新機能:

- 以下の機能のサポートを追加しました。
  - MADセンシングやNCSI/IPMI OEMコマンドに関する温度しきい値の高/低デフォルト。

- user_mtuのサイズをファームウェアに示す"set port"コマンドに新しいフィールドの追加。
- ファームウェアが内部QPで受信されたパケットを落としたり、WQEプロデューサーフェッチングを使用不可にすることを確認する保護メカニズム。

ファームウェアバージョン2.40.5072での新機能:

- Platform Level Data Model(PLDM)のサポート。

ファームウェアバージョン2.42.5000での新機能:

- 以下の機能のサポートを追加しました。
  - 新しいTLV:CX3_GLOBAL_CONFを使用して、mlxconfig構成を介して着信パケットのタイムスタンプを有効または無効にします。
  - ユーザーMAC構成。
  - ドライバーのリセット前に自動的にmstdumpを収集します。
  - TPT(iron)からDEAD_IRISC(plastic)を検出し、アサートを発生させるメカニズム。
  - user_mtuのサイズをファームウェアに示す"set port"コマンドに新しいフィールドの追加。
- コマンドタイムアウトの場合のデバッグ機能が向上しました。

オンラインファームウェアアップグレードユーティリティ (Windows x64) for HPE Mellanox VPI (EthernetおよびInfinibandモード)デバイス - Windows x86_64プラットフォーム

バージョン: 1.0.0.6 (A) **(推奨)**
ファイル名: cp037179.compsig; cp037179.exe

修正

バージョン2.40.5030および2.40.5072での修正:

- ドライバーの起動中にファームウェアとハードウェアの競合が発生し、送信の完了がブロックされました。
- そのファームウェアはclose_portコマンドを実行している間、ドライバーにlink_downイベントを送りませんでした。

バージョン2.42.5000での修正:

- PortRcvPktsカウンターはリセット後にクリアされませんでした。
- 10個を超える仮想ファンクションがFLRを実行し、完了タイムアウト値が16ミリ秒より小さい範囲に構成されている場合に、仮想ファンクション(VF)の構成サイクルでシステムのタイムアウトが発生する問題。
- ドライバーを(別のスレッドから)並行して再起動しているときに、"mlxfwtop –d mt4103_pci_cr0"を実行した場合、サーバーがハングしてNMIになります。この場合、デバイスのダウンストリームブリッジは完了タイムアウトエラーを報告しました。
- bmc_rebootの実行後にBMCがIPv6でpingを受信できなかったflow_steeringの問題。
- HCAを閉じている間、RXパケットは存在しなかったリソースへの不正アクセスを引き起こし、その結果QPCGWまたはiriscがスタックしました。
- ポートがActiveやArmedの状態でない場合に、マスターSMLIDとLIDが0または0xFFFFである問題。
- ibdumpがすべてのMADパケットをキャプチャーできない問題。
- 再起動後にリンクアップしませんでした。
- sw_resetの実行中に到着したPCIeコンフィギュレーションサイクルが2つの完了を生成する原因となる、まれな問題を修正しました。
- iniファイル内にdisable_stat-ic_steering_iniフィールドを追加したときに、スクラッチパッドでのこのフィールドのメモリ割り当ての問題により、ネットワークコントローラー サイドバンドインターフェイス(NC-SI)が動作しなくなる問題。

バージョン2.42.5004での修正:

- UEFI(Unified Extensible Firmware Interface)HII(ヒューマンインターフェイスインフラストラクチャ)メニューでは、HPE Gen10デバイスを使用すると、両方のポートがポート1として表示されます。
- UEFI(Unified Extensible Firmware Interface)のブートメニューで、HPE Gen10デバイスを使用すると、デバイス名に不要なポート番号が表示されます。

拡張

次のデバイス用のファームウェアが2.40.5030にアップデートされました。
764286-B21
778509-B21

次のデバイス用のファームウェアが2.40.5072にアップデートされました。
764285-B21

次のデバイス用のファームウェアが2.42.5004にアップデートされます。
764283-B21
764284-B21

次のデバイス用のファームウェアが2.42.5000にアップデートされます。
764282-B21

ファームウェアバージョン2.40.5030での新機能:

- 以下の機能のサポートを追加しました。
  - MADセンシングやNCSI/IPMI OEMコマンドに関する温度しきい値の高/低デフォルト。
  - user_mtuのサイズをファームウェアに示す"set port"コマンドに新しいフィールドの追加。
  - ファームウェアが内部QPで受信されたパケットを落としたり、WQEプロヂューサーフェッチングを使用不可にすることを確認する保護メカニズム。

ファームウェアバージョン2.40.5072での新機能:

- Platform Level Data Model(PLDM)のサポート。

ファームウェアバージョン2.42.5000での新機能:

- 以下の機能のサポートを追加しました。
  - 新しいTLV: CX3_GLOBAL_CONFを使用して、mlxconfig構成を介して着信パケットのタイムスタンプを有効または無効にします。
  - ユーザーMAC構成。
  - ドライバーのリセット前に自動的にmstdumpを収集します。
  - TPT(iron)からDEAD_IRISC(plastic)を検出し、アサートを発生させるメカニズム。
  - user_mtuのサイズをファームウェアに示す"set port"コマンドに新しいフィールドの追加。
- コマンドタイムアウトの場合のデバッグ機能が向上しました。

オンラインファームウェアアップグレードユーティリティ(ESXi 6.0) for HPE Mellanox Ethernetアダプター専用

バージョン: 1.0.8 **(推奨)**
ファイル名: CP034531.compsig; CP034531.zip

重要な注意！

FWバージョン2.42.5000 での既知の問題:

- mlxconfigを使用してcq_timestampを有効または無効にすることはサポートされていません。
- 2つの別個のLEDスキーム(Phy LEDと論理LED)を備えたカードでは、Phy LEDだけが点灯します。つまり、オレンジ色のLEDは、ETHリンクがアイドルモードの間はアクティブではありません。
- SR-IOVセットアップでは、PFがVMに渡されるときにmlxconfigを使用すると、ハイパーバイザーの再起動を必要とします。
- 前のGAにダウングレードするにはサーバーのリブートが必要です。v2.30.8000以降のバージョンから2.30.8000より前のバージョンにダウングレードするには、サーバーのリブートが必要です。サーバーを再起動します。
- ConnectX-3 Ethernet アダプターカードでは、ファームウェア管理ツールによって返されるGUID値とデバイスファームウェアを通してGUIDを読み込むファブリック/ドライバーユーティリティ(例えば、ibstatを使用)によって返される値の間にミスマッチがあります。ユーティリティがMACアドレスから得られた値を返すとき、Mlxburn/flintはGUIDとして0xffffを返します。すべてのドライバー/ファームウェア/ソフトウェアのために、後者の値が使用されるべきです。
- SBRはConnectX®-3アダプターのために最低50msアサートされる必要があります
- Pilot1 SL230で、PCIeリンクは時々Gen3の速度に達しません。
- ドライバーの互換性の問題のため、SR-IOVがVPIカードで有効になっている場合、RH6.3インボックスドライバーがカーネルパニックを引き起こします。

- アドバンストステアリングモードで、MCGごとに8以上のQPを持つ場合、サイドバンド管理接続性が失われることがあります。
- システムBIOSでSR-IOVが無効にされたとき、Linuxカーネルv3.8のUbuntu v12.04.3で、Mellanoxを含むいくつかの製造業者のNICが動作しない可能性があるPCI問題が認識されています。
- MFTツールは、ツール動作が停止を強制された場合にロックされたフラッシュセマフォを残すことがありました。セマフォがロックされていると、ファームウェアはフラッシュにアクセスすることができず、ハングアップします。
- MC2210411-SR4モジュールを使用する場合、ケーブル情報MADは正しくないケーブル情報をレポートします。
- 10C/分以上のスピードで温度が上昇するとGen2が故障します(MT27518A1-FDIR-BVのみ)。
- MT27518A1-FDIR-BVでは10C/分以上のスピードで温度が上昇するとPCIe Gen2リンクが不安定になります。
- Bloomフィルターは、現在サポートされません。
- ファームウェアダウングレードメッセージ ファームウェアv2.11.0000からダウングレードし、MFT 3.0.0-3を使用する場合
- MLNX_OFED-2.0.3でInfiniBandを使用する場合、RM＃DMFSを有効にしないでください
- RM#VPD読み取り専用のフィールドが書き込み可能です。
- SymbolErrorCounterの増加 ポート1 FDRとポート2 40Gを使用してVPIモードで動作すると、エラーカウンターが誤動作して急激に増加します
- デバイスを128Byte CQ/EQストライドに設定するとサイドバンド管理が正常に機能せず、コミュニケーション消失につながります。
- CQおよびEQを異なるストライドサイズに構成することはできません。
- ConnectX-3 Pro VFデバイスIDは、ドライバーの制限のためのConnectX-3 VFデバイスIDと同じように示されます。
- PXE (レガシー)をG9サーバーで稼働中のRSOD。これはPXEブートに失敗し、BIOSがHDDからブートするときにのみ起こります。現在BIOSの修正は保留中です。
- ポートがETHスイッチに接続されているときに、NCSI/IPMIが有効になっている状態でポートプロトコルをETHからIBに変更することは推奨されません。
- IPv6上でのRDPは、現在機能しません。
- Sniffer QP では、"push to that rule"と同等の挿入スキームのあるQPを追加した後に正規のルールを削除できません。
- PCI Physical FunctionごとのBoot Entry Vector (BEV)のみがサポートされているので、最初のポートを無効化すると、二番目のポートも消えてしまいます。
- NICは、56GbEポートリンクのNICポートからケーブルが外れてしまっている場合に、リンクダウンをドライバーに通知しません。
- 100GbE 光ケーブルを使用している場合に、56GbE リンクが起動しません。
- MLNX_OFED v3.3-1.0.0.0を使用している場合、サーバーのリブートが非同期イベントハンドラーから呼ばれたmlx-4_en_get_drvinfo() のカーネルパニックにより、動けなくなることがあります。
- 832298: ibdumpを実行しているとき、ループバックトラフィックがカーネルドライバーにミラーリングされます。
- AHSが誤ったMTUサイズをレポートします
- RM#846523: ifconfigを使用してOSから設定されたMACアドレスがOCBBバッファーに反映されません。

FWバージョン14.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。
- mlxconfigツールが、既存の拡張ROMイメージだけを表示するのでなく、可能なすべての拡張ROMイメージを表示します。
- nic_receive_steering_discard コマンドを実行しているとき、イーサーネットマルチキャストループバックパケットがカウントされません(ローカルループバックパケットでなくても)。
- デュアルポートVHCAが非ネイティブポートでRoCEパケットを送信し、パケットが系列のvport FDBに到達すると、パケットソースvportが一致するルールで不一致が起きる場合があります。

FWバージョン12.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- まれに、署名がされた再送信/パケット損失が原因でエラーが発生し、接続が終了することがあります。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。
- mlxconfigツールが、既存の拡張ROMイメージだけを表示するのでなく、可能なすべての拡張ROMイメージを表示します。
- nic_receive_steering_discard コマンドを実行しているとき、イーサーネットマルチキャストループバックパケットがカウントされません(ローカルループバックパケットでなくても)。

- デュアルポートVHCAが非ネイティブポートでRoCEパケットを送信し、パケットが系列のvport FDBに到達すると、パケットソースvportが一致するルールで不一致が起きる場合があります。
- DC CNAKストレステスト中に、DC CNAKタイムアウト(CNAKドロップ)が発生することがあります。

FWバージョン16.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。

事前要件

HPE Synergy 6410C 25/50Gb Ethernetアダプター(868779-B21)を先に前提となるファームウェアバージョン12.21.2808にアップグレードしてから、12.22.0148または12.22.0194にアップデートする必要があります。
12.22.0194は、HPE Synergy 6410C 25/50Gb Ethernetアダプター(868779-B21)の初のセキュアファームウェアです。いったんこのデバイスをファームウェア12.22.0194にアップグレードすると、ダウングレードができません。

修正

バージョン2.42.5000で提出された修正:

- PortRcvPktsカウンターがリセット後にクリアされない問題を解決しました。
- 10個を超える仮想関数がFLRを実行し、完了タイムアウト値が
- 16ミリ秒より小さい範囲に構成されている場合に、VFの構成サイクルでシステムのタイムアウトが発生する問題を修正しました。
- ドライバーを(別のスレッドから)並行して再起動しているときに、"mlxfwtop –d mt4103_pci_cr0"を実行した場合、サーバーがハングしてNMIになるという問題を修正しました。この場合、デバイスのダウンストリームブリッジは完了タイムアウトエラーを報告しました。
- bmc_rebootの実行後にBMCがIPV6でpingを受信できなかったflow_steeringの問題を修正しました。
- 存在しないリソースに対してRXパケットが不正なアクセスを引き起こし、その結果QPCGWまたはiriscがスタックする、HCAを閉じる際の問題を修正しました。
- ポートがActiveやArmedの状態でない場合に、masterSM LIDとLIDが0または0xFFFFである問題を修正しました。
- ibdumpがすべてのMADパケットをキャプチャーできない問題を修正しました。
- リブート後にリンクが上がらないという問題を修正しました。
- sw_resetの実行中に到着したPCIeコンフィギュレーションサイクルが2つの完了を生成する原因となる、まれな問題を修正しました。
- iniファイル内にdisable_static_steering_iniフィールドを追加したときに、スクラッチパッドでのこのフィールドのメモリ割り当ての問題により、NC-SIが動作しなくなる問題を修正しました。

バージョン14.22.1414 で提出された修正:

- 温度正規化関数の計算問題。純粋整数ではないケーブルゲインの考慮を修正しました。
- 応答で異なる構造の原因になっていたASNのオブジェクト0x8のパーサーに関連する問題を修正しました。
- スタンバイモードでのリブート時にバックプレーンポートケージが意図せず電源オフになることを回避するためのオプションを追加しました。
- LAGが有効な場合にvportの状態をクエリするときに、ドライバーが2つの物理ポートの誤った論理ORを返す原因となる問題を修正しました。
- EDRリンク結果を向上するため、フルワイヤスピード(FWS)しきい値を大きくしました。
- アフィニティQPがオープンの状態でVFがFLRを受信した場合に、"Destroy LAG"コマンドが失敗する問題。
- RoCEデュアルポートモードが有効になっている場合、2番目のポートでtcpdumpが機能しません。

拡張

次のデバイス用のファームウェアが2.42.5000にアップデートされます。

779799-B21 (HP Ethernet 10Gb 2-port 546FLR-SFP+ アダプター)
779793-B21 (HP Ethernet 10Gb 2-port 546SFP+ アダプター)

バージョン2.42.5000の新機能および変更:

- 以下の機能のサポートを追加しました。
  - TLV:CX3_GLOBAL_CONFを使用して、mlxconfig構成を介して着信パケットのタイムスタンプを有効または無効にします。
  - ユーザーMAC構成。
  - ドライバーのリセット前に自動的にmstdumpを収集します。
  - TPT(iron)からDEAD_IRISC(plastic)を検出し、アサートを発生させます。
- コマンドタイムアウトの場合のデバッグ機能を強化しました。
- user_mtuのサイズをファームウェアに示す「set port」 コマンドに新しいコマンドを追加しました。

次のデバイス用のファームウェアが14.22.1414にアップデートされます:

817749-B21 (HPE Ethernet 25Gb 2-port 640FLR-SFP28アダプター)
817753-B21 (HPE Ethernet 25Gb 2-port 640SFP28アダプター)

バージョン14.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **ソフトウェアのリセットフロー:**致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **破棄パケットのステアリングカウンター:**廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **仮想機能(VF):**PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで58 VF
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。
- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- **vportミラーリング:**パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性:特殊なエラーイベント:**QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。
- QPの作成時間を高速化しました。
- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

次のデバイス用のファームウェアが12.22.1414にアップデートされました:

868779-B21(HPE Synergy 6410C 25/50Gb Ethernetアダプター)

バージョン12.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **ソフトウェアのリセットフロー:**致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **破棄パケットのステアリングカウンター:**廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **仮想機能(VF):**PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで58 VF
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。
- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- **vportミラーリング:**パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性:特殊なエラーイベント:**QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。

- QPの作成時間を高速化しました。
- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

次のデバイス用のファームウェアが16.22.1414にアップデートされました:

874253-B21(HPE Ethernet 100Gb 1-port 842QSFP28アダプター)

バージョン16.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **ソフトウェアのリセットフロー:**致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **破棄パケットのステアリングカウンター:**廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。
- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- Push/Pop VLAN、新しいFLOW TABLE ENTRYアクションのサポートを追加します。これらの新しい操作は、Q-in-Q機能を実装する、ドライバーによって使用されます。
- ConnectX 5 アダプターカードでパケット ペーシングします。
- **vportミラーリング:**パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性:特殊なエラーイベント:**QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。
- QPの作成時間を高速化しました。
- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

サポートしているデバイスおよび機能

HPE部品番号	InfiniBandカードタイプ	PSID
779793-B21	HP Ethernet 10Gb 2ポート546SFP+アダプター	HP_1200111023
779799-B21	HP Ethernet 10Gb 2ポート546FLR-SFP+アダプター	HP_2240110004
817749-B21	HPE Ethernet 25Gb 2ポート 640FLR-SFP28 アダプター	HP_2690110034
817753-B21	HPE Ethernet 25Gb 2ポート 640SFP28 アダプター	HP_2420110034
868779-B21	HPE Synergy 6410C 25/50Gb Ethernetアダプター	HPE0000000006
874253-B21	HPE Ethernet 100Gb 1ポート 842QSFP28 アダプター	HPE0000000014

オンラインファームウェアアップグレードユーティリティ(Linux x86_64) for HPE Mellanox Ethernetアダプター専用

バージョン: 1.0.8 (A) **(推奨)**

ファイル名: 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

重要な注意！

FWバージョン2.42.5000 での既知の問題:

- mlxconfigを使用してcq_timestampを有効または無効にすることはサポートされていません。
- 2つの別個のLEDスキーム(Phy LEDと論理LED)を備えたカードでは、Phy LEDだけが点灯します。つまり、オレンジ色のLEDは、ETHリンクがアイドルモードの間はアクティブではありません。
- SR-IOVセットアップでは、PFがVMに渡されるときにmlxconfigを使用すると、ハイパーバイザーの再起動を必要とします。
- 前のGAにダウングレードするにはサーバーのリブートが必要です。v2.30.8000以降のバージョンから2.30.8000より前のバージョンにダウングレードするには、サーバーのリブートが必要です。サーバーを再起動します。
- ConnectX-3 Ethernet アダプターカードでは、ファームウェア管理ツールによって返されるGUID値とデバイスファームウェアを通してGUIDを読み込むファブリック/ドライバーユーティリティ(例えば、ibstatを使用)によって返される値の間にミスマッチがあります。ユーティリティがMACアドレスから得られた値を返すとき、Mlxburn/flintはGUIDとして0xffffを返します。すべてのドライバー/ファームウェア/ソフトウェアのために、後者の値が使用されるべきです。
- SBRはConnectX®-3アダプターのために最低50msアサートされる必要があります
- Pilot1 SL230で、PCIeリンクは時々Gen3の速度に達しません。
- ドライバーの互換性の問題のため、SR-IOVがVPIカードで有効になっている場合、RH6.3インボックスドライバーがカーネルパニックを引き起こします。
- アドバンストステアリングモードで、MCGごとに8以上のQPを持つ場合、サイドバンド管理接続性が失われることがあります。
- システムBIOSでSR-IOVが無効にされたとき、Linuxカーネルv3.8のUbuntu v12.04.3で、Mellanoxを含むいくつかの製造業者のNICが動作しない可能性があるPCI問題が認識されています。
- MFTツールは、ツール動作が停止を強制された場合にロックされたフラッシュセマフォを残すことがありました。セマフォがロックされていると、ファームウェアはフラッシュにアクセスすることができず、ハングアップします。
- MC2210411-SR4モジュールを使用する場合、ケーブル情報MADは正しくないケーブル情報をレポートします。
- 10C/分以上のスピードで温度が上昇するとGen2が故障します(MT27518A1-FDIR-BVのみ)。
- MT27518A1-FDIR-BVでは10C/分以上のスピードで温度が上昇するとPCIe Gen2リンクが不安定になります。
- Bloomフィルターは、現在サポートされません。
- ファームウェアダウングレードメッセージ ファームウェアv2.11.0000からダウングレードし、MFT 3.0.0-3を使用する場合
- MLNX_OFED-2.0.3でInfiniBandを使用する場合、RM＃DMFSを有効にしないでください
- RM#VPD読み取り専用のフィールドが書き込み可能です。
- SymbolErrorCounterの増加 ポート1 FDRとポート2 40Gを使用してVPIモードで動作すると、エラーカウンターが誤動作して急激に増加します
- デバイスを128Byte CQ/EQストライドに設定するとサイドバンド管理が正常に機能せず、コミュニケーション消失につながります。
- CQおよびEQを異なるストライドサイズに構成することはできません。
- ConnectX-3 Pro VFデバイスIDは、ドライバーの制限のためのConnectX-3 VFデバイスIDと同じように示されます。
- PXE (レガシー)をG9サーバーで稼働中のRSOD。これはPXEブートに失敗し、BIOSがHDDからブートするときにのみ起こります。現在BIOSの修正は保留中です。
- ポートがETHスイッチに接続されているときに、NCSI/IPMIが有効になっている状態でポートプロトコルをETHからIBに変更することは推奨されません。
- IPv6上でのRDPは、現在機能しません。
- Sniffer QP では、"push to that rule"と同等の挿入スキームのあるQPを追加した後に正規のルールを削除できません。
- PCI Physical FunctionごとのBoot Entry Vector (BEV)のみがサポートされているので、最初のポートを無効化すると、二番目のポートも消えてしまいます。
- NICは、56GbEポートリンクのNICポートからケーブルが外れてしまっている場合に、リンクダウンをドライバーに通知しません。
- 100GbE 光ケーブルを使用している場合に、56GbE リンクが起動しません。
- MLNX_OFED v3.3-1.0.0.0を使用している場合、サーバーのリブートが非同期イベントハンドラーから呼ばれたmlx4_en_get_drvinfo() のカーネルパニックにより、動けなくなることがあります。
- 832298: ibdumpを実行しているとき、ループバックトラフィックがカーネルドライバーにミラーリングされます。
- AHSが誤ったMTUサイズをレポートします
- RM#846523: ifconfigを使用してOSから設定されたMACアドレスがOCBBバッファーに反映されません。

FWバージョン14.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。
- mlxconfigツールが、既存の拡張ROMイメージだけを表示するのでなく、可能なすべての拡張ROMイメージを表示します。
- nic_receive_steering_discard コマンドを実行しているとき、イーサーネットマルチキャストループバックパケットがカウントされません(ローカルループバックパケットでなくても)。
- デュアルポートVHCAが非ネイティブポートでRoCEパケットを送信し、パケットが系列のvport FDBに到達すると、パケットソースvportが一致するルールで不一致が起きる場合があります。

FWバージョン12.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- まれに、署名がされた再送信/パケット損失が原因でエラーが発生し、接続が終了することがあります。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。
- mlxconfigツールが、既存の拡張ROMイメージだけを表示するのでなく、可能なすべての拡張ROMイメージを表示します。
- nic_receive_steering_discard コマンドを実行しているとき、イーサーネットマルチキャストループバックパケットがカウントされません(ローカルループバックパケットでなくても)。
- デュアルポートVHCAが非ネイティブポートでRoCEパケットを送信し、パケットが系列のvport FDBに到達すると、パケットソースvportが一致するルールで不一致が起きる場合があります。
- DC CNAKストレステスト中に、DC CNAKタイムアウト(CNAKドロップ)が発生することがあります。

FWバージョン16.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。

事前要件

HPE Synergy 6410C 25/50Gb Ethernetアダプター(868779-B21)を先に前提となるファームウェアバージョン12.21.2808にアップグレードしてから、12.22.0148または12.22.0194にアップデートする必要があります。
12.22.0194は、HPE Synergy 6410C 25/50Gb Ethernetアダプター(868779-B21)の初のセキュアファームウェアです。いったんこのデバイスをファームウェア12.22.0194にアップグレードすると、ダウングレードができません。

修正

バージョン2.42.5000で提出された修正:

- PortRcvPktsカウンターはリセット後にクリアされませんでした。
- 10個を超える仮想ファンクションがFLRを実行し、完了タイムアウト値が16ミリ秒より小さい範囲に構成されている場合に、VFの構成サイクルでシステムのタイムアウトが発生する問題。
- ドライバーを(別のスレッドから)並行して再起動しているときに、"mlxfwtop –d mt4103_pci_cr0"を実行した場合、サーバーがハングしてNMI(マスク不可能割り込み)になる問題。この場合、デバイスのダウンストリームブリッジは完了タイムアウトエラーを報告しました。
- bmc_rebootの実行後にBMCがIPv6でpingを受信できなかったflow_steeringの問題。
- 存在しないリソースに対してRXパケットが不正なアクセスを引き起こし、その結果QPCGWまたはiriscがスタックする、HCA(ホストチャネルアダプター)を閉じる際の問題。
- ポートがActiveやArmedの状態でない場合に、マスターSMLIDとLIDが0または0xFFFFである問題。
- ibdumpがすべてのMADパケットをキャプチャーできない問題。
- 再起動後にリンクアップしませんでした。
- sw_resetの実行中に到着したPCIeコンフィギュレーションサイクルが2つの完了を生成する原因となる、まれな問題。
- iniファイル内にdisable_stat-ic_steering_iniフィールドを追加したときに、スクラッチパッドでのこのフィールドのメモリ割り当ての問題により、NC-SI(Network Controller Sideband Interface)が動作しなくなる問題。

バージョン14.22.1414 で提出された修正:

- 温度正規化関数の計算問題。純粋整数ではないケーブルゲインの考慮を修正しました。
- 応答で異なる構造の原因になっていたASNのオブジェクト0x8のパーサーに関連する問題を修正しました。

- スタンバイモードでのリブート時にバックプレーンポートケージが意図せず電源オフになることを回避するためのオプションを追加しました。
- LAGが有効な場合にvportの状態をクエリするときに、ドライバーが2つの物理ポートの誤った論理ORを返す原因となる問題を修正しました。
- EDRリンク結果を向上するため、フルワイヤスピード(FWS)しきい値を大きくしました。
- アフィニティQPがオープンの状態でVFがFLRを受信した場合に、"Destroy LAG"コマンドが失敗する問題。
- RoCEデュアルポートモードが有効になっている場合、2番目のポートでtcpdumpが機能しません。

拡張

次のデバイス用のファームウェアが2.42.5000にアップデートされます。

779799-B21 (HP Ethernet 10Gb 2-port 546FLR-SFP+ アダプター)
779793-B21 (HP Ethernet 10Gb 2-port 546SFP+ アダプター)

バージョン2.42.5000の新機能および変更:

- 以下の機能のサポートを追加しました。
  - TLV: CX3_GLOBAL_CONFを使用して、mlxconfig構成を介して着信パケットのタイムスタンプを有効または無効にします。
  - ユーザーMAC構成。
  - ドライバーのリセット前に自動的にmstdumpを収集します。
  - TPT(iron)からDEAD_IRISC(plastic)を検出し、アサートを発生させます。
- コマンドタイムアウトの場合のデバッグ機能を強化しました。
- user_mtuのサイズをファームウェアに示す「set port」 コマンドに新しいコマンドを追加しました。

次のデバイス用のファームウェアが14.22.1414にアップデートされます:

817749-B21 (HPE Ethernet 25Gb 2-port 640FLR-SFP28アダプター)
817753-B21 (HPE Ethernet 25Gb 2-port 640SFP28アダプター)

バージョン14.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **ソフトウェアのリセットフロー:** 致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **破棄パケットのステアリングカウンター:** 廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **仮想ファンクション(VF):**PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで58 VF
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。
- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- **vportミラーリング:** パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性: 特殊なエラーイベント:**QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。
- QPの作成時間を高速化しました。
- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

次のデバイス用のファームウェアが12.22.1414にアップデートされました:

868779-B21(HPE Synergy 6410C 25/50Gb Ethernetアダプター)

バージョン12.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **ソフトウェアのリセットフロー:** 致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **破棄パケットのステアリングカウンター:** 廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
    - nic_receive_steering_discard
    - receive_discard_vport_down
    - transmit_discard_vport_down
- **仮想ファンクション(VF):**PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
    - デュアルポートデバイスで20 VF
    - 単一ポートデバイスで58 VF
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。
- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- **vportミラーリング:** パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性: 特殊なエラーイベント:**QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。
- QPの作成時間を高速化しました。
- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

次のデバイス用のファームウェアが16.22.1414にアップデートされました:

874253-B21(HPE Ethernet 100Gb 1-port 842QSFP28アダプター)

バージョン16.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **ソフトウェアのリセットフロー:** 致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **破棄パケットのステアリングカウンター:** 廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
    - nic_receive_steering_discard
    - receive_discard_vport_down
    - transmit_discard_vport_down
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。
- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- Push/Pop VLAN、新しいFLOW TABLE ENTRYアクションのサポートを追加します。これらの新しい操作は、Q-in-Q機能を実装する、ドライバーによって使用されます。
- ConnectX 5 アダプターカードでパケット ペーシングします。
- **vportミラーリング:** パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性: 特殊なエラーイベント:**QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。
- QPの作成時間を高速化しました。
- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

サポートしているデバイスおよび機能

HPE部品番号	InfiniBandカードタイプ	PSID
779793-B21	HP Ethernet 10Gb 2ポート546SFP+アダプター	HP_1200111023
779799-B21	HP Ethernet 10Gb 2ポート546FLR-SFP+アダプター	HP_2240110004
817749-B21	HPE Ethernet 25Gb 2ポート 640FLR-SFP28 アダプター	HP_2690110034
817753-B21	HPE Ethernet 25Gb 2ポート 640SFP28 アダプター	HP_2420110034
868779-B21	HPE Synergy 6410C 25/50Gb Ethernetアダプター	HPE0000000006
874253-B21	HPE Ethernet 100Gb 1ポート 842QSFP28 アダプター	HPE0000000014

オンラインファームウェアアップグレードユーティリティ(Windows x64) for HPE Mellanox Ethernetアダプター専用

バージョン: 1.0.0.8 (B) **(推奨)**
ファイル名: cp037168.compsig; cp037168.exe

重要な注意！

FWバージョン2.42.5000 での既知の問題:

- mlxconfigを使用してcq_timestampを有効または無効にすることはサポートされていません。
- 2つの別個のLEDスキーム(Phy LEDと論理LED)を備えたカードでは、Phy LEDだけが点灯します。つまり、オレンジ色のLEDは、ETHリンクがアイドルモードの間はアクティブではありません。
- SR-IOVセットアップでは、PFがVMに渡されるときにmlxconfigを使用すると、ハイパーバイザーの再起動を必要とします。
- 前のGAにダウングレードするにはサーバーのリブートが必要です。v2.30.8000以降のバージョンから2.30.8000より前のバージョンにダウングレードするには、サーバーのリブートが必要です。サーバーを再起動します。
- ConnectX-3 Ethernet アダプターカードでは、ファームウェア管理ツールによって返されるGUID値とデバイスファームウェアを通してGUIDを読み込むファブリック/ドライバーユーティリティ(例えば、ibstatを使用)によって返される値の間にミスマッチがあります。ユーティリティがMACアドレスから得られた値を返すとき、Mlxburn/flintはGUIDとして0xffffを返します。すべてのドライバー/ファームウェア/ソフトウェアのために、後者の値が使用されるべきです。
- SBRはConnectX®-3アダプターのために最低50msアサートされる必要があります
- Pilot1 SL230で、PCIeリンクは時々Gen3の速度に達しません。
- ドライバーの互換性の問題のため、SR-IOVがVPIカードで有効になっている場合、RH6.3インボックスドライバーがカーネルパニックを引き起こします。
- アドバンストステアリングモードで、MCGごとに8以上のQPを持つ場合、サイドバンド管理接続性が失われることがあります。
- システムBIOSでSR-IOVが無効にされたとき、Linuxカーネルv3.8のUbuntu v12.04.3で、Mellanoxを含むいくつかの製造業者のNICが動作しない可能性があるPCI問題が認識されています。
- MFTツールは、ツール動作が停止を強制された場合にロックされたフラッシュセマフォを残すことがありました。セマフォがロックされていると、ファームウェアはフラッシュにアクセスすることができず、ハングアップします。
- MC2210411-SR4モジュールを使用する場合、ケーブル情報MADは正しくないケーブル情報をレポートします。
- 10C/分以上のスピードで温度が上昇するとGen2が故障します(MT27518A1-FDIR-BVのみ)。
- MT27518A1-FDIR-BVでは10C/分以上のスピードで温度が上昇するとPCIe Gen2リンクが不安定になります。
- Bloomフィルターは、現在サポートされません。
- ファームウェアダウングレードメッセージ ファームウェアv2.11.0000からダウングレードし、MFT 3.0.0-3を使用する場合
- MLNX_OFED-2.0.3でInfiniBandを使用する場合、RM＃DMFSを有効にしないでください
- RM#VPD読み取り専用のフィールドが書き込み可能です。
- SymbolErrorCounterの増加 ポート1 FDRとポート2 40Gを使用してVPIモードで動作すると、エラーカウンターが誤動作して急激に増加します
- デバイスを128Byte CQ/EQストライドに設定するとサイドバンド管理が正常に機能せず、コミュニケーション消失につながります。
- CQおよびEQを異なるストライドサイズに構成することはできません。
- ConnectX-3 Pro VFデバイスIDは、ドライバーの制限のためのConnectX-3 VFデバイスIDと同じように示されます。
- PXE (レガシー)をG9サーバーで稼働中のRSOD。これはPXEブートに失敗し、BIOSがHDDからブートするときにのみ起こります。現在BIOSの修正は保留中です。

- ポートがETHスイッチに接続されているときに、NCSI/IPMIが有効になっている状態でポートプロトコルをETHからIBに変更することは推奨されません。
- IPv6上でのRDPは、現在機能しません。
- Sniffer QP では、"push to that rule"と同等の挿入スキームのあるQPを追加した後に正規のルールを削除できません。
- PCI Physical FunctionごとのBoot Entry Vector (BEV)のみがサポートされているので、最初のポートを無効化すると、二番目のポートも消えてしまいます。
- NICは、56GbEポートリンクのNICポートからケーブルが外れてしまっている場合に、リンクダウンをドライバーに通知しません。
- 100GbE 光ケーブルを使用している場合に、56GbE リンクが起動しません。
- MLNX_OFED v3.3-1.0.0.0を使用している場合、サーバーのリブートが非同期イベントハンドラーから呼ばれたmlx-4_en_get_drvinfo() のカーネルパニックにより、動けなくなることがあります。
- 832298: ibdumpを実行しているとき、ループバックトラフィックがカーネルドライバーにミラーリングされます。
- AHSが誤ったMTUサイズをレポートします
- RM#846523: ifconfigを使用してOSから設定されたMACアドレスがOCBBバッファーに反映されません。

FWバージョン14.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。
- mlxconfigツールが、既存の拡張ROMイメージだけを表示するのでなく、可能なすべての拡張ROMイメージを表示します。
- nic_receive_steering_discard コマンドを実行しているとき、イーサーネットマルチキャストループバックパケットがカウントされません(ローカルループバックパケットでなくても)。
- デュアルポートVHCAが非ネイティブポートでRoCEパケットを送信し、パケットが系列のvport FDBに到達すると、パケットソースvportが一致するルールで不一致が起きる場合があります。

FWバージョン12.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- まれに、署名がされた再送信/パケット損失が原因でエラーが発生し、接続が終了することがあります。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。
- mlxconfigツールが、既存の拡張ROMイメージだけを表示するのでなく、可能なすべての拡張ROMイメージを表示します。
- nic_receive_steering_discard コマンドを実行しているとき、イーサーネットマルチキャストループバックパケットがカウントされません(ローカルループバックパケットでなくても)。
- デュアルポートVHCAが非ネイティブポートでRoCEパケットを送信し、パケットが系列のvport FDBに到達すると、パケットソースvportが一致するルールで不一致が起きる場合があります。
- DC CNAKストレステスト中に、DC CNAKタイムアウト(CNAKドロップ)が発生することがあります。

FWバージョン16.22.1414での既知の問題:

- フックで負の温度を設定すると、PLDMセンサー読み取りコマンドを実行しているときに誤ったセンサー状態がレポートされます。
- ヘルスカウンターが10msごとでなく50msごとに大きくなります。

事前要件

HPE Synergy 6410C 25/50Gb Ethernetアダプター(868779-B21)を先に前提となるファームウェアバージョン12.21.2808にアップグレードしてから、12.22.0148または12.22.0194にアップデートする必要があります。
12.22.0194は、HPE Synergy 6410C 25/50Gb Ethernetアダプター(868779-B21)の初のセキュアファームウェアです。いったんこのデバイスをファームウェア12.22.0194にアップグレードすると、ダウングレードができません。

修正

バージョン2.42.5000で提出された修正:

- PortRcvPktsカウンターがリセット後にクリアされない問題を解決しました。
- 10個を超える仮想関数がFLRを実行し、完了タイムアウト値が

- 16ミリ秒より小さい範囲に構成されている場合に、VFの構成サイクルでシステムのタイムアウトが発生する問題を修正しました。
- ドライバーを(別のスレッドから)並行して再起動しているときに、"mlxfwtop –d mt4103_pci_cr0"を実行した場合、サーバーがハングしてNMIになるという問題を修正しました。この場合、デバイスのダウンストリームブリッジは完了タイムアウトエラーを報告しました。
- bmc_rebootの実行後にBMCがIPV6でpingを受信できなかったflow_steeringの問題を修正しました。
- 存在しないリソースに対してRXパケットが不正なアクセスを引き起こし、その結果QPCGWまたはiriscがスタックする、HCAを閉じる際の問題を修正しました。
- ポートがActiveやArmedの状態でない場合に、masterSM LIDとLIDが0または0xFFFFである問題を修正しました。
- ibdumpがすべてのMADパケットをキャプチャーできない問題を修正しました。
- リブート後にリンクが上がらないという問題を修正しました。
- sw_resetの実行中に到着したPCIeコンフィギュレーションサイクルが2つの完了を生成する原因となる、まれな問題を修正しました。
- iniファイル内にdisable_static_steering_iniフィールドを追加したときに、スクラッチパッドでのこのフィールドのメモリ割り当ての問題により、NC-SIが動作しなくなる問題を修正しました。

バージョン14.22.1414 で提出された修正:

- 温度正規化関数の計算問題。純粋整数ではないケーブルゲインの考慮を修正しました。
- 応答で異なる構造の原因になっていたASNのオブジェクト0x8のパーサーに関連する問題を修正しました。
- スタンバイモードでのリブート時にバックプレーンポートケージが意図せず電源オフになることを回避するためのオプションを追加しました。
- LAGが有効な場合にvportの状態をクエリするときに、ドライバーが2つの物理ポートの誤った論理ORを返す原因となる問題を修正しました。
- EDRリンク結果を向上するため、フルワイヤスピード(FWS)しきい値を大きくしました。
- アフィニティQPがオープンの状態でVFがFLRを受信した場合に、"Destroy LAG"コマンドが失敗する問題。
- RoCEデュアルポートモードが有効になっている場合、2番目のポートでtcpdumpが機能しません。

拡張

次のデバイス用のファームウェアが2.42.5000にアップデートされます。

779799-B21 (HP Ethernet 10Gb 2-port 546FLR-SFP+ アダプター)
779793-B21 (HP Ethernet 10Gb 2-port 546SFP+ アダプター)

バージョン2.42.5000の新機能および変更:

- 以下の機能のサポートを追加しました。
  - TLV: CX3_GLOBAL_CONFを使用して、mlxconfig構成を介して着信パケットのタイムスタンプを有効または無効にします。
  - ユーザーMAC構成。
  - ドライバーのリセット前に自動的にmstdumpを収集します。
  - TPT(iron)からDEAD_IRISC(plastic)を検出し、アサートを発生させます。
- コマンドタイムアウトの場合のデバッグ機能を強化しました。
- user_mtuのサイズをファームウェアに示す「set port」 コマンドに新しいコマンドを追加しました。

次のデバイス用のファームウェアが14.22.1414にアップデートされます:

817749-B21 (HPE Ethernet 25Gb 2-port 640FLR-SFP28アダプター)
817753-B21 (HPE Ethernet 25Gb 2-port 640SFP28アダプター)

バージョン14.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **ソフトウェアのリセットフロー:** 致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **破棄パケットのステアリングカウンター:** 廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down

- **仮想ファンクション(VF):**PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで58 VF
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。
- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- **vportミラーリング:** パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性: 特殊なエラーイベント:**QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。
- QPの作成時間を高速化しました。
- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

次のデバイス用のファームウェアが12.22.1414にアップデートされました:

868779-B21(HPE Synergy 6410C 25/50Gb Ethernetアダプター)

バージョン12.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **ソフトウェアのリセットフロー:** 致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **破棄パケットのステアリングカウンター:** 廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- **仮想ファンクション(VF):**PFあたりのフルVMQoS(8 TC)で動作できるVFの数が次のように増加しました
  - デュアルポートデバイスで20 VF
  - 単一ポートデバイスで58 VF
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。
- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- **vportミラーリング:** パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性: 特殊なエラーイベント:**QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。
- QPの作成時間を高速化しました。
- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

次のデバイス用のファームウェアが16.22.1414にアップデートされました:

874253-B21(HPE Ethernet 100Gb 1-port 842QSFP28アダプター)

バージョン16.22.1414の新機能および変更:

- 4MBから7Mファームウェアイメージバンクへの移行。
- **ソフトウェアのリセットフロー:** 致命的なエラーのソフトウェア検出、ソフトウェアによる将来のデバッグに備えたmstdumpファイルの自動作成、およびデバイスのリセット。
- **破棄パケットのステアリングカウンター:** 廃棄パケットを(vport別に)カウントするために次のカウンターが追加されました
  - nic_receive_steering_discard
  - receive_discard_vport_down
  - transmit_discard_vport_down
- Pause Frame DurationおよびXOFF Resend Timeが仕様で定義されている最大値へと増加しました。

- **PCI Relax Ordering:**mlxconfig構成で強制的なPCI Relax Orderingをmkey_contextで有効化または無効化できるようになりました。
- Push/Pop VLAN、新しいFLOW TABLE ENTRYアクションのサポートを追加します。これらの新しい操作は、Q-in-Q機能を実装する、ドライバーによって使用されます。
- ConnectX 5 アダプターカードでパケット ペーシングします。
- **vportミラーリング:** パケットは、特定のミラーリングポリシーに基づいてミラー化されます。ポリシーは、ACLテーブルの転送アクション(イングレス/イーグレス)をサポートする「set FTEコマンド」を使用して設定されます。
- **耐障害性: 特殊なエラーイベント:**QSFPケージに接続されている10GBaseTモジュールのサポートを追加しました。
- QPの作成時間を高速化しました。
- SR-IOVのデフォルトルーティングモードがLIDベースになりました。mlxconfigツールによる構成の変更が可能になりました。
- 追加のConnectX-4 LxアダプターカードにPXEとUEFIを追加しました。ConnectX-4 LxがPXE、x86-UEFI、およびArm-UEFIを保持するようになりました。

サポートしているデバイスおよび機能

HPE部品番号	InfiniBandカードタイプ	PSID
779793-B21	HP Ethernet 10Gb 2ポート546SFP+アダプター	HP_1200111023
779799-B21	HP Ethernet 10Gb 2ポート546FLR-SFP+アダプター	HP_2240110004
817749-B21	HPE Ethernet 25Gb 2ポート 640FLR-SFP28 アダプター	HP_2690110034
817753-B21	HPE Ethernet 25Gb 2ポート 640SFP28 アダプター	HP_2420110034
868779-B21	HPE Synergy 6410C 25/50Gb Ethernetアダプター	HPE0000000006
874253-B21	HPE Ethernet 100Gb 1ポート 842QSFP28 アダプター	HPE0000000014

ファームウェア - NVDIMM

先頭

Linux用オンラインフラッシュコンポーネント - 16GB NVDIMM-N DDR4-2666

バージョン: 1.04 **(推奨)**
ファイル名: 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

修正

最初のリリース。

拡張

最初のリリース。

Windows x64用オンラインフラッシュコンポーネント - 16GB NVDIMM-N DDR4-2666

バージョン: 1.04 **(推奨)**
ファイル名: cp032705.compsig; cp032705.exe

修正

最初のリリース。

拡張

最初のリリース。

ファームウェア - PCIe NVMeストレージディスク

先頭

Linux(x64)サプリメンタルアップデート/オンラインROMフラッシュコンポーネント - MK000400KWDUK, VK000480KWDUE、MK000800KWDUL、VK000960KWDUF、MK001600KWDUN、およびVK001920KWDUHドライブ

バージョン: HPK2 **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります。**

事前要件

HPE NVMe PCIeソリッドステートドライブが、オンラインファームウェアアップデートで以下のOSバージョンを必要とします。

- 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

修正

修正された問題点:

- HPE ProLiant BL460c Gen10サーバーのブート操作中に、ストレージコントローラーによってドライブが検出されませんでした。

Windows用オンラインROMフラッシュコンポーネント(x64)- MK000400KWDUK、VK000480KWDUE、MK000800KWDUL、VK000960KWDUF、MK001600KWDUN、およびVK001920KWDUHドライブ

バージョン: HPK2 **(推奨)**
ファイル名: cp033283.compsig; cp033283.exe; cp033283.md5

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります。**

修正

修正された問題点:

- HPE ProLiant BL460c Gen10サーバーのブート操作中に、ストレージコントローラーによってドライブが検出されませんでした。

拡張

改善点/新しい機能:

- 消耗ステータスおよび温度情報を提供するためのヘルスデータの取得が改善されました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - LO0400KEFJQ、LO0800KEFJR、LO1600KEFJT、LO2000KEFJU、LT0800KEXVA、LT1600KEXVB、およびLT2000KEXVCドライブ

バージョン: HPK4 **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-d64642c780-HPK4-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-d64642c780-HPK4-1.1.x86_64.rpm

事前要件

HPE NVMe PCIeソリッドステートドライブは、以下の最低限のOSレベルがオンラインファームウェアアップデートで必要になります。

- Red Hat Enterprise Linux 7.4。
- SUSE Linux Enterprise Server 12 SP3。
- SUSE Linux Enterprise Server 11 SP4。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- MO0400KEFHN、MO0800KEFHP、MO1600KEFHQ、MO2000KEFHR、MT0800KEXUU、およびMT1600KEXUVドライブ

バージョン: HPK4 **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-2a5b65f157-HPK4-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-2a5b65f157-HPK4-1.1.x86_64.rpm

事前要件

HPE NVMe PCIeソリッドステートドライブは、以下の最低限のOSレベルがオンラインファームウェアアップデートで必要になります。

- Red Hat Enterprise Linux 7.4。
- SUSE Linux Enterprise Server 12 SP3。
- SUSE Linux Enterprise Server 11 SP4。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- VO0400KEFJB、VO1200KEFJC、およびVO2000KEFJDドライブ

バージョン: HPK4 **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-9a826ccd8a-HPK4-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-9a826ccd8a-HPK4-1.1.x86_64.rpm

事前要件

HPE NVMe PCIeソリッドステートドライブは、以下の最低限のOSレベルがオンラインファームウェアアップデートで必要になります。

- Red Hat Enterprise Linux 7.4。
- SUSE Linux Enterprise Server 12 SP3。
- SUSE Linux Enterprise Server 11 SP4。

ファームウェア - パワーマネジメント

先頭

オンラインROMフラッシュ for Linux - Power Management Controller

バージョン: 4.1 (E) **(推奨)**
ファイル名: RPMS/i386/hp-firmware-powerpic-dl580-4.1-5.i386.rpm

重要な注意！

重要な注意:

Ver. 4.1 (E)はファームウェアRPMインストールコマンド名の"cpqsetup"から"hpsetup"への変更を含んでいて、機能的にVer. 4.1と同等です。ファームウェアをバージョン4.1にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョンEにアップグレードする必要はありません。

提供名:

Power Management Controller

リリースバージョン:

4.1 (E)

最新の推奨またはクリティカルリビジョン:

これは、このファームウェアでの最初のバージョンです。

以前のリビジョン:

これは、このファームウェアでの最初のバージョンです。

ファームウェアの関連性:

なし

改善点/新しい機能:

これは、このファームウェアでの最初のバージョンです。

修正された問題点:

なし

既知の問題点:

インストール手順が完了すると、スマートコンポーネントが不必要なリブートを促します。アップデートの効果とハードウェアの安定を得るために、インストール後のリブートは必要ありません。

事前要件

このフラッシュコンポーネントを使用する前に、"HP ProLiant iLO 3/4 Channel Interface Driver"がインストールされて実行されている必要があります。 ドライバーが実行されていない場合、次のエラーメッセージが表示されます。
「The software is not supported for installation on this system.
You must install the iLO Channel Interface driver to use this component.」

拡張

重要な注意:

バージョン4.1 (E)は、"cpqsetup"から"hpsetup"へのファームウェアRPMインストールコマンド名の変更を含んでいて、機能的にバージョン4.1と同じです。ファームウェアをバージョン4.1にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョンEにアップグレードする必要はありません。

ファームウェアの関連性:

なし

改善点/新しい機能:

これは、このファームウェアでの最初のバージョンです。

既知の問題点:

インストール手順が完了すると、スマートコンポーネントが不必要なリブートを促します。 アップデートの効果とハードウェアの安定を得るために、インストール後のリブートは必要ありません。

オンラインROMフラッシュ for Linux - アドバンスト消費電力上限マイクロコントローラーファームウェア for HPE Gen10サーバー

バージョン: 1.0.4 **(推奨)**
ファイル名: 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

重要な注意！

重要な注意:

なし

提供名:

HPE Gen10サーバー用アドバンストパワーキャッピングマイクロコントローラーファームウェア

リリースバージョン:

1.0.4

最新の推奨またはクリティカルリビジョン:

1.0.4

以前のリビジョン:

1.0.2

ファームウェアの依存関係:

Integrated Lights-Out 5(iLO 5)ファームウェアバージョン1.15およびシステムROMバージョン1.20以降

改善点/新しい機能:

動的消費電力上限のサポートの追加 適切に動作するために、Integrated Lights-Out 5(iLO 5)ファームウェアバージョン1.15およびシステムROMバージョン1.20以降がサーバー上で更新されていることを確認してください。

修正された問題点:

なし

既知の問題点:

なし

事前要件

スタンダードLinuxカーネルに含まれているLinux用"iLO 5 Channel Interface Driver"(CHIF)。

Integrated Lights-Out 5(iLO 5)ファームウェアバージョン1.15およびシステムROMバージョン1.20以降

拡張

重要な注意:

なし

ファームウェアの依存関係:

Integrated Lights-Out 5(iLO 5)ファームウェアバージョン1.15およびシステムROMバージョン1.20以降

改善点/新しい機能:

動的消費電力上限のサポートの追加 適切に動作するために、Integrated Lights-Out 5(iLO 5)ファームウェアバージョン1.15およびシステムROMバージョン1.20以降がサーバー上で更新されていることを確認してください。

既知の問題点:

なし

オンラインROMフラッシュ for Linux - アドバンスト消費電力上限マイクロコントローラーファームウェア for HPE Gen9サーバー

バージョン: 1.0.9 (F) **(オプション)**
ファイル名: RPMS/i386/hp-firmware-powerpic-gen9-1.0.9-6.1.i386.rpm

重要な注意！

重要な注意:

Ver. 1.0.9 (F) には新しいサーバー製品のサポートが含まれます。機能的にVer. 1.0.9と同等です。ファームウェアをバージョン1.0.9にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョンFにアップグレードする必要はありません。

提供名:

アドバンストパワーキャッピングマイクロコントローラーファームウェア(HPE Gen9サーバー)

リリースバージョン:

1.0.9

最新の推奨またはクリティカルリビジョン:

1.0.7

以前のリビジョン:

1.0.7

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

最小消費電力上限値が特定のシステムで誤って計算されていた問題に対処しました。この修正により、POST中の最小上限値設定の正確さが向上します。

既知の問題点:

なし

事前要件

このフラッシュコンポーネントを使用する前に、"HP ProLiant iLO 3/4 Channel Interface Driver"がインストールされて実行されている必要があります。 ドライバーが実行されていない場合、次のエラーメッセージが表示されます。
「The software is not supported for installation on this system.
You must install the iLO Channel Interface driver to use this component.」

修正

重要な注意:

Ver. 1.0.9 (F) には新しいサーバー製品のサポートが含まれます。機能的にVer. 1.0.9と同等です。ファームウェアをバージョン1.0.9にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョンFにアップグレードする必要はありません。

ファームウェアの依存関係:

なし

修正された問題点:

最小消費電力上限値が特定のシステムで誤って計算されていた問題に対処しました。この修正により、POST中の最小上限値設定の正確さが向上します。

既知の問題点:

なし

オンラインROMフラッシュ for VMware ESXi - Power Management Controller

バージョン: 4.1 (E) **(推奨)**
ファイル名: CP026094.zip

重要な注意！

重要な注意:

Ver. 4.1 (E)はコンポーネントパッケージのアップデートを含んでいて、機能的にVer. 4.1と同等です。 ファームウェアをバージョン4.1にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョンEにアップグレードする必要はありません。

提供名:

Power Management Controller

リリースバージョン:

4.1(E)

最新の推奨またはクリティカルリビジョン:

これは、このファームウェアでの最初のバージョンです。

以前のリビジョン:

これは、このファームウェアでの最初のバージョンです。

ファームウェアの関連性:

なし

改善点/新しい機能:

これは、このファームウェアでの最初のバージョンです。

修正された問題点:

なし

既知の問題点:

インストール手順が完了すると、スマートコンポーネントが不必要なリブートを促します。 アップデートの効果とハードウェアの安定を得るために、インストール後のリブートは必要ありません。

事前要件

このフラッシュコンポーネントを使用する前に、"HP ProLiant iLO 3/4 Channel Interface Driver"がインストールされて実行されている必要があります。 ドライバーが実行されていない場合、次のエラーメッセージが表示されます。
「The software is not supported for installation on this system.
You must install the iLO Channel Interface driver to use this component.」

拡張

重要な注意:

Ver. 4.1 (E)はコンポーネントパッケージのアップデートを含んでいて、機能的にVer. 4.1と同等です。 ファームウェアをバージョン4.1にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョンEにアップグレードする必要はありません。

ファームウェアの関連性:

なし

改善点/新しい機能:

これは、このファームウェアでの最初のバージョンです。

既知の問題点:

インストール手順が完了すると、スマートコンポーネントが不必要なリブートを促します。 アップデートの効果とハードウェアの安定を得るために、インストール後のリブートは必要ありません。

オンラインROMフラッシュ for VMware ESXi - アドバンスト消費電力上限マイクロコントローラーファームウェア for HPE Gen9サーバー

バージョン: 1.0.9 (F) **(オプション)**
ファイル名: CP031168.zip

重要な注意！

重要な注意:

Ver. 1.0.9 (F) には新しいサーバー製品のサポートが含まれます。 機能的にVer. 1.0.9と同等です。 ファームウェアをバージョン1.0.9にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョンFにアップグレードする必要はありません。

提供名:

アドバンストパワーキャッピングマイクロコントローラーファームウェア(HPE Gen9サーバー)

リリースバージョン:

1.0.9

最新の推奨またはクリティカルリビジョン:

1.0.7

以前のリビジョン:

1.0.7

ファームウェアの依存関係:

なし

改善点/新しい機能:

なし

修正された問題点:

最小消費電力上限値が特定のシステムで誤って計算されていた問題に対処しました。 この修正により、POST中の最小上限値設定の正確さが向上します。

既知の問題点:

なし

事前要件

このコンポーネントは、実行する前に以下のHPEドライバーがロードされている必要があります。

1. "HPE ProLiant iLO 3/4 Channel Interface Driver" (CHIF) をインストールされて稼動している必要があります。

ESXi 5.1、5.5およびESXi 6.0、6.5の最小iLOバージョンは1.4です。

2. "Compaq ROM Utility Driver" (CRU) をインストールされて稼動している必要があります。

ESXi 5.1の最小CRUバージョンは5.0.3.9です。

ESXi 5.5の最小CRUバージョンは5.5.4.1です。

ESXi 6.0の最小CRUバージョンは6.0.8です。

6.5の最小CRUバージョンは6.5.8です。

両方のドライバーがHPE VMware Custom Imageに統合されます。これは他のHPEの高度な管理ツールにも含まれます。 ドライバーは、vibsdepot.hpe.comのVMware vSphere 6.5、6.0、5.5および5.1用のOS固有の"HPE Agentless Management Service Offline Bundle"からも入手できます。

修正

重要な注意:

Ver. 1.0.9 (F) には新しいサーバー製品のサポートが含まれます。機能的にVer. 1.0.9と同等です。ファームウェアをバージョン1.0.9にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョンFにアップグレードする必要はありません。

ファームウェアの依存関係:

なし

修正された問題点:

最小消費電力上限値が特定のシステムで誤って計算されていた問題に対処しました。この修正により、POST中の最小上限値設定の正確さが向上します。

既知の問題点:

なし

拡張

なし

オンラインROMフラッシュ for Windows x64 - アドバンスト消費電力上限マイクロコントローラーファームウェア for HPE Gen9サーバー

バージョン: 1.0.9 (H) **(オプション)**
ファイル名: cp034944.exe

重要な注意！

重要な注意:

バージョン1.0.9 (H) には、情報漏えいの脆弱性の問題(CVE-2017-8992)を解決するためのアップデートが含まれています。機能的にVer. 1.0.9と同等です。 ファームウェアをバージョン1.0.9にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョン(H)にアップグレードする必要はありません。

提供名:

アドバンストパワーキャッピングマイクロコントローラーファームウェア(HPE Gen9サーバー)

リリースバージョン:

1.0.9

最新の推奨またはクリティカルリビジョン:

1.0.7

以前のリビジョン:

1.0.7

ファームウェアの依存関係:

なし

改善点/新しい機能:

Microsoft Windows 10(64-bit)のサポートを追加しました

修正された問題点:

最小消費電力上限値が特定のシステムで誤って計算されていた問題に対処しました。この修正により、POST中の最小上限値設定の正確さが向上します。

既知の問題点:

なし

事前要件

このフラッシュコンポーネントを使用する前に、"Windows向けHPE ProLiant iLO 3/4 Channel Interface Driver"がインストールされて実行されている必要があります。 ドライバーが実行されていない場合、次のエラーメッセージが表示されます。
「The software is not supported for installation on this system.
You must install the iLO Channel Interface driver to use this component.」

修正

重要な注意:

Ver. 1.0.9 (G) には新しいサーバー製品のサポートが含まれます。 機能的にVer. 1.0.9と同等です。 ファームウェアをバージョン1.0.9にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョン(G)にアップグレードする必要はありません。

ファームウェアの依存関係:

なし

修正された問題点:

最小消費電力上限値が特定のシステムで誤って計算されていた問題に対処しました。この修正により、POST中の最小上限値設定の正確さが向上します。

既知の問題点:

なし

拡張

Microsoft Windows 10(64-bit)のサポートを追加しました

オンラインROMフラッシュ for Windows x64 - Power Management Controller

バージョン: 4.1 (E) **(推奨)**
ファイル名: cp035154.exe

重要な注意！

重要な注意:

バージョン4.1 (E)には、情報漏えいの脆弱性の問題(CVE-2017-8992)を解決するためのアップデートが含まれています。 機能的にバージョン4.1と同等です。 ファームウェアをバージョン4.1にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョン(E)にアップグレードする必要はありません。

提供名:

Power Management Controller

リリースバージョン:

4.1 (E)

最新の推奨またはクリティカルリビジョン:

これは、このファームウェアでの最初のバージョンです。

以前のリビジョン:
これは、このファームウェアでの最初のバージョンです。

ファームウェアの依存関係:

なし

改善点/新しい機能:

これは、このファームウェアでの最初のバージョンです。

修正された問題点:

なし

インストール手順が完了すると、スマートコンポーネントが不必要なリブートを促します。アップデートの効果とハードウェアの安定を得るために、インストール後のリブートは必要ありません。

事前要件

このフラッシュコンポーネントを使用する前に、"HP ProLiant iLO 3/4 Channel Interface Driver for Windows"がインストールされて実行されている必要があります。 ドライバーが実行されていない場合、次のエラーメッセージが表示されます。
「The software is not supported for installation on this system.
You must install the iLO Channel Interface driver to use this component.」

拡張

重要な注意:

Ver. 4.1(D)は、HP Smart Update ManagerのOSインストールサポートへのアップデートを含みます。 Ver. 4.1(D)に含まれているPower Management Controllerファームウェアは、Ver. 4.1と同一です。 そのため、Power Management Controllerファームウェアが4.1の場合、4.1(D)にアップグレードする必要はありません。

ファームウェアの関連性:

なし

改善点/新しい機能:

これは、このファームウェアでの最初のバージョンです。

既知の問題点:

インストール手順が完了すると、スマートコンポーネントが不必要なリブートを促します。 アップデートの効果とハードウェアの安定を得るために、インストール後のリブートは必要ありません。

オンラインROMフラッシュ for Windows x64 - アドバンスト消費電力上限マイクロコントローラーファームウェア for HPE Gen10サーバー

バージョン: 1.0.4 (B) **(推奨)**
ファイル名: cp034430.compsig; cp034430.exe

重要な注意！

重要な注意:

Ver. 1.0.4 (B)には新しいサーバー製品のサポートが含まれます。 機能的にVer. 1.0.4と同等です。 ファームウェアをバージョン1.0.4にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョン(B)にアップグレードする必要はありません。

提供名:

HPE Gen10サーバー用アドバンストパワーキャッピングマイクロコントローラーファームウェア

リリースバージョン:

1.0.4

最新の推奨またはクリティカルリビジョン:

1.0.4

以前のリビジョン:

1.0.2

ファームウェアの依存関係:

Integrated Lights-Out 5(iLO 5)ファームウェアバージョン1.15およびシステムROMバージョン1.20以降

改善点/新しい機能:

動的消費電力上限のサポートの追加 適切に動作するために、Integrated Lights-Out 5(iLO 5)ファームウェアバージョン1.15およびシステムROMバージョン1.20以降がサーバー上で更新されていることを確認してください。

Microsoft Windows 10(64-bit)のサポートを追加しました

修正された問題点:

なし

既知の問題点:

なし

事前要件

Service Pack for ProLiant(SPP)から入手可能なWindows用のiLO 5 Channel Interface Driver(CHIF)。

Integrated Lights-Out 5(iLO 5)ファームウェアバージョン1.15およびシステムROMバージョン1.20以降。

拡張

重要な注意:

Ver. 1.0.4 (B)には新しいサーバー製品のサポートが含まれます。 機能的にVer. 1.0.4と同等です。 ファームウェアをバージョン1.0.4にアップグレードするために以前のリビジョンのコンポーネントが使われた場合は、リビジョン(B)にアップグレードする必要はありません。

ファームウェアの依存関係:

Integrated Lights-Out 5(iLO 5)ファームウェアバージョン1.15およびシステムROMバージョン1.20以降

改善点/新しい機能:

動的消費電力上限のサポートの追加 適切に動作するために、Integrated Lights-Out 5(iLO 5)ファームウェアバージョン1.15およびシステムROMバージョン1.20以降がサーバー上で更新されていることを確認してください。

Microsoft Windows 10(64-bit)のサポートを追加しました

既知の問題点:

なし

ファームウェア - SASストレージディスク

先頭

Linux (x64) - EH000300JWCPK、EH000600JWCPL、およびEH000900JWCPNドライブ用サプリメンタルアップデート / オンラインROMフラッシュコンポーネント

バージョン: HPD3 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD3を既にインストールしている場合、HPD3 (B) へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

Linux (x64) 用サプリメンタルアップデート / オンラインROMフラッシュコンポーネント- EG000300JWFVB ドライブ

バージョン: HPD2 **(オプション)**
ファイル名: 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

修正

- このファームウェアにより、一部の設定がMicrosoft Storage Spaces認証要件に適合するよう変更されます。

拡張

- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

Linux (x64)用サプリメンタルアップデート / オンラインROMフラッシュコンポーネント - EH000600JWCPFおよび EH000900JWCPHドライブ

バージョン: HPD4 **(推奨)**
ファイル名: 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

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

Linux (x64)用サプリメンタルアップデート / オンラインROMフラッシュコンポーネント- EG000600JWFUVおよびEG001200JWFVA ドライブ

バージョン: HPD3 **(オプション)**
ファイル名: 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

修正

- このファームウェアにより、一部の設定がMicrosoft Storage Spaces認証要件に適合するよう変更されます。

拡張

- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

Linux (x64)用サプリメンタルアップデート / オンラインROMフラッシュコンポーネント- EG000600JWJNP and EG001200JWJNQドライブ

バージョン: HPD1 **(推奨)**
ファイル名: 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

修正

- このファームウェアには、特定の順次書き込み中にタイムアウトエラーが発生する可能性のあるまれなケースの問題についての修正が含まれています。ランダム書き込みワークロード中に応答時間が長くなる問題の修正があります。

拡張

- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

Linux (x64)用サプリメンタルアップデート / オンラインROMフラッシュコンポーネント-EG001800JWJNRおよびEG002400JWJNTドライブ

バージョン: HPD1 **(推奨)**
ファイル名: 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

修正

- このファームウェアには、特定の順次書き込み中にタイムアウトエラーが発生する可能性のあるまれなケースの問題についての修正が含まれています。ランダム書き込みワークロード中に応答時間が長くなる問題の修正があります。

拡張

- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

Linux(x64)用サプリメンタルアップデート/オンラインROMフラッシュコンポーネント - EG0300FCSPH、EG0450FCSPK、EG0600FCSPL、およびEG0900FCSPNドライブ

バージョン: HPD2 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD2を既にインストールしている場合、HPD2(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

VMware ESXi用オンラインROMフラッシュコンポーネント - EG001800JWFVCドライブ

バージョン: HPD2 (C) **(推奨)**
ファイル名: CP036118.compsig; CP036118.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを**

使用したオフライン更新が必要です。
- **ファームウェアバージョンHPD2を既にインストールしている場合、HPD2(C)へ更新する必要はありません。**

修正

- このファームウェアアップデートでは、アラインされていないWRITEおよびVERIFYコマンドが不良セクターに送信されたときのデータの整合性のリスクが排除されます。これらの条件の間、ディスクに書き込まれるように意図されたデータの書き込みが失敗する可能性があります。

VMware ESXi用オンラインROMフラッシュコンポーネント - EH000600JWCPFおよびEH000900JWCPHドライブ

バージョン: HPD4 (B) **(推奨)**
ファイル名: CP036127.compsig; CP036127.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD4を既にインストールしている場合、HPD4(B)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。
- このファームウェアには、キュー深度が小さいシーケンシャルライトワークロード時にパフォーマンスが低下する場合の修正が含まれています。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

VMware ESXi用オンラインROMフラッシュコンポーネント - MB4000JEXYAおよびMB6000JEXYBドライブ

バージョン: HPD8 (C) **(推奨)**
ファイル名: CP036153.compsig; CP036153.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD8を既にインストールしている場合、HPD8(C)へ更新する必要はありません。**

修正

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.

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

VMware ESXi用オンラインROMフラッシュコンポーネント- EG000300JWFVBドライブ

バージョン: HPD2 (B) **(オプション)**
ファイル名: CP036114.compsig; CP036114.zip

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**

修正

- このファームウェアにより、一部の設定がMicrosoft Storage Spaces認証要件に適合するよう変更されます。

VMware ESXi用オンラインROMフラッシュコンポーネント- EG000600JWFUVおよびEG001200JWFVAドライブ

バージョン: HPD3 (B) **(オプション)**
ファイル名: CP036116.compsig; CP036116.zip

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**

修正

- このファームウェアにより、一部の設定がMicrosoft Storage Spaces認証要件に適合するよう変更されます。

VMware ESXi用オンラインROMフラッシュコンポーネント- EG000600JWJNPおよびEG001200JWJNQドライブ

バージョン: HPD1 (B) **(推奨)**
ファイル名: CP036117.compsig; CP036117.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**

- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**

修正

- このファームウェアには、特定の順次書き込み中にタイムアウトエラーが発生する可能性のあるまれなケースの問題についての修正が含まれています。ランダム書き込みワークロード中に応答時間が長くなる問題の修正があります。

VMware ESXi用オンラインROMフラッシュコンポーネント- EG001800JWJNRおよびEG002400JWJNTドライブ

バージョン: HPD1 (B) **(推奨)**
ファイル名: CP036119.compsig; CP036119.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**

修正

- このファームウェアには、特定の順次書き込み中にタイムアウトエラーが発生する可能性のあるまれなケースの問題についての修正が含まれています。ランダム書き込みワークロード中に応答時間が長くなる問題の修正があります。

Windows (x64)用オンラインROMフラッシュコンポーネント EH000300JWCPK、EH000600JWCPL、およびEH000900JWCPNドライブ

バージョン: HPD3 (B) **(推奨)**
ファイル名: cp034310.compsig; cp034310.exe; cp034310.md5

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- Windows Server 2016 Device Guardのサポートを追加しました。

Windows(64)用オンラインROMフラッシュコンポーネント - EG001800JWFVCドライブ

バージョン: HPD2 (B) **(推奨)**
ファイル名: cp035543.compsig; cp035543.exe; cp035543.md5

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**
- **ファームウェアバージョンHPD2を既にインストールしている場合、HPD2(B)へアップデートする必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

Windows用 (x64) オンラインROMフラッシュコンポーネント- EG000600JWFUVおよびEG001200JWFVA ドライブ

バージョン: HPD3 **(オプション)**
ファイル名: cp035614.compsig; cp035614.exe; cp035614.md5

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります。**

修正

- このファームウェアにより、一部の設定がMicrosoft Storage Spaces認証要件に適合するよう変更されます。

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

Windows用(x64)オンラインROMフラッシュコンポーネント- EG000600JWJNPおよびEG001200JWJNQドライブ

バージョン: HPD1 **(推奨)**
ファイル名: cp035603.compsig; cp035603.exe; cp035603.md5

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**

修正

- このファームウェアには、特定の順次書き込み中にタイムアウトエラーが発生する可能性のあるまれなケースの問題についての修正が含まれています。ランダム書き込みワークロード中に応答時間が長くなる問題の修正があります。

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

Windows用(x64)オンラインROMフラッシュコンポーネント- EG001800JWJNRおよびEG002400JWJNTドライブ

バージョン: HPD1 **(推奨)**
ファイル名: cp035599.compsig; cp035599.exe; cp035599.md5

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**

修正

- このファームウェアには、特定の順次書き込み中にタイムアウトエラーが発生する可能性のあるまれなケースの問題についての修正が含まれています。ランダム書き込みワークロード中に応答時間が長くなる問題の修正があります。

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MO0200JEFNV、MO0400JEFPA、MO0800JEFPB、MO1600JEFPC、EO0200JEFPD、EO0400JEFPE、およびEO0800JEFPFドライブ

バージョン: HPD3 (C) **(推奨)**
ファイル名: CP036169.compsig; CP036169.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD3を既にインストールしている場合、HPD3(C)へ更新する必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - EG000600JWEBHおよびEG000300JWEBFドライブ

バージョン: HPD3 (C) **(推奨)**
ファイル名: CP036115.compsig; CP036115.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD3を既にインストールしている場合、HPD3(C)へ更新する必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - EG0300JEHLV、EG0600JEHMA、EG0900JEHMB、およびEG1200JEHMCドライブ

バージョン: HPD5 (D) **(推奨)**
ファイル名: CP036121.compsig; CP036121.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD5を既にインストールしている場合、HPD5(D)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - EG0300JFCKA、EG0600JEMCV、EG0900JFCKB、およびEG1200JEMDAドライブ

バージョン: HPD6 (C) **(推奨)**
ファイル名: CP036122.compsig; CP036122.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD6を既にインストールしている場合、HPD6(C)へ更新する必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - EG1800JEHMDドライブ

バージョン: HPD6 (D) **(推奨)**
ファイル名: CP036124.compsig; CP036124.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD6を既にインストールしている場合、HPD6(D)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - EG1800JEMDBドライブ

バージョン: HPD5 (B) **(推奨)**
ファイル名: CP036125.compsig; CP036125.zip

修正

- このファームウェアには、キュー深度が小さいシーケンシャルライトワークロード時にパフォーマンスが低下する場合の修正が含まれています。
- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - EH000300JWCPK、EH000600JWCPL、およびEH000900JWCPNドライブ

バージョン: HPD3 (C) **(推奨)**
ファイル名: CP036128.compsig; CP036128.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD3を既にインストールしている場合、HPD3(C)へ更新する必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - EH0300JDYTH、 EH0450JDYTK、およ

び EH0600JDYTLドライブ

バージョン: HPD6 (D) **(推奨)**
ファイル名: CP036130.compsig; CP036130.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD6を既にインストールしている場合、HPD6(D)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - EH0300JEDHC、EH0450JEDHD、およびEH0600JEDHEドライブ

バージョン: HPD4 (D) **(推奨)**
ファイル名: CP036131.compsig; CP036131.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD4を既にインストールしている場合、HPD4(D)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - EO000400JWDKP、EO000800JWDKQ、EO001600JWDKR、MO000400JWDKU、MO000800JWDKV、MO001600JWDLA、およびMO003200JWDLBドライブ

バージョン: HPD1 (C) **(推奨)**
ファイル名: CP036132.compsig; CP036132.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD1を既にインストールしている場合、HPD1(C)へ更新する必要はありません。**

修正

- UNMAPコマンドのサポートを削除しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB010000JWAYKおよびMB008000JWAYHドライブ

バージョン: HPD5 **(クリティカル)**
ファイル名: CP036862.compsig; CP036862.zip

修正

- このコードは、アラインされていない書込みコマンドに関連する潜在的なデータの完全性の問題を修正します。これらの問題は、サプライヤーの継続的なラボテスト中でのみ検出されました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB2000JFDSLおよびMB4000JFDSNドライブ

バージョン: HPD4 (C) **(推奨)**
ファイル名: CP036146.compsig; CP036146.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD4を既にインストールしている場合、HPD4(C)へ更新する必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB2000JFEMLおよびMB4000JFEMNドライブ

バージョン: HPD6 (C) **(クリティカル)**
ファイル名: CP036147.compsig; CP036147.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**

- **ファームウェアバージョンHPD6を既にインストールしている場合、HPD6(C)へ更新する必要はありません。**

修正

- プロセス中の書き込みの再試行が誤った場所で間違って開始されることによって発生する潜在的なデータ整合性の問題を修正します。 これらの問題は、サプライヤーの継続的な信頼性テスト中で検出されました。
- ファームウェアは、緊急の電源オフの改善も含まれます。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB2000JFEPAおよびMB4000JFEPBドライブ

バージョン: HPD5 (C) **(推奨)**
ファイル名: CP036148.compsig; CP036148.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD5を既にインストールしている場合、HPD5(C)へ更新する必要はありません。**

修正

修正された問題点:

- ファームウェアには、ドライブがアクティブからアイドルAに移行する時にコマンドを受け取った場合に、Windowsでの通常コマンド完了時間が4～5秒になるのを防ぐための変更が含まれます。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB4000JEFNCおよびMB6000JEFNDドライブ

バージョン: HPD9 (C) **(推奨)**
ファイル名: CP036151.compsig; CP036151.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD9を既にインストールしている場合、HPD9(C)へ更新する必要はありません。**

修正

修正された問題点:

- このファームウェアには、パフォーマンスに影響を与える可能性のあるドライブリセットの問題を回避するための変更が含まれています。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB4000JEQNLおよびMB6000JEQNNドライブ

バージョン: HPDB (C) **(推奨)**
ファイル名: CP036152.compsig; CP036152.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPDBを既にインストールしている場合、HPDB(C)へ更新する必要はありません。**

修正

- プロセス中の書き込みの再試行が誤った場所で間違って開始されることによって発生する潜在的なデータ整合性の問題を修正します。 これらの問題は、サプライヤーの継続的な信頼性テスト中で検出されました。
- ファームウェアは、緊急の電源オフの改善も含まれます。

拡張

拡張機能/新機能

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB6000JEQUVおよびMB8000JEQVAドライブ

バージョン: HPDB (C) **(推奨)**
ファイル名: CP036158.compsig; CP036158.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPDBを既にインストールしている場合、HPDB(C)へ更新する必要はありません。**

修正

修正された問題点:

- このファームウェアは、書き込みエラー回復プロセス中に発生する潜在的なタイムアウトを改善し(ドライブを内部的にリセットさせる)、可能性のあるデータ管理上の問題を修正します。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB6000JVYZDおよびMB4000JVYZCドライブ

バージョン: HPD3 (B) **(推奨)**
ファイル名: CP036160.compsig; CP036160.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD3を既にインストールしている場合、HPD3(B) へアップデートする必要はありません。**

修正

- このファームウェアには、ドライブがMicrosoft Azureスタック認証の要件を満たせるようになる変更が含まれています。 さらに、特定の順次書き込み中にタイムアウトエラーが発生する可能性のあるまれなケースの問題についての修正も含まれています。

オンラインROMフラッシュコンポーネント for VMware ESXi - MM1000JEFRBおよびMM2000JEFRCドライブ

バージョン: HPD8 (B) **(オプション)**
ファイル名: CP036167.compsig; CP036167.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD8を既にインストールしている場合、HPD8(B)へアップデートする必要はありません。**

修正

- このファームウェアにより、ドライブはAzureスタック認証の要件を満たすことができます。
- このファームウェアには、VPD 80ページに報告されているドライブシリアル番号の変更が含まれています。ドライブラベルで表示されているのと同じように報告されます。 削除されたあらゆる文字が空白のプレースホルダーに置き換えられるので、ログの形式は変わりません。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MM1000JFJTHドライブ

バージョン: HPD3 (B) **(オプション)**
ファイル名: CP036168.compsig; CP036168.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD3を既にインストールしている場合、HPD3(B) へアップデートする必要はありません。**

修正

- このファームウェアにより、ドライブはAzureスタック認証の要件を満たすことができます。
- このファームウェアには、VPD 80ページに報告されているドライブシリアル番号の変更が含まれています。ドライブラベルで表示されているのと同じように報告されます。 削除されたあらゆる文字が空白のプレースホルダーに置き換えられるので、ログの形式は変わりません。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - VO1920JEUQQドライブ

バージョン: HPD3 (C) **(推奨)**
ファイル名: CP036176.compsig; CP036176.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD3を既にインストールしている場合、HPD3(C)へ更新する必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MO0200JEFNV、MO0400JEFPA、MO0800JEFPB、MO1600JEFPC、EO0200JEFPD、EO0400JEFPE、およびEO0800JEFPFドライブ

バージョン: HPD3 (B) **(推奨)**
ファイル名: cp034334.compsig; cp034334.exe; cp034334.md5

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - EG000300JWFVB ドライブ

バージョン: HPD2 **(オプション)**
ファイル名: cp035611.compsig; cp035611.exe; cp035611.md5

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります。**

修正

- このファームウェアにより、一部の設定がMicrosoft Storage Spaces認証要件に適合するよう変更されます。

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - EG000600JWEBHおよびEG000300JWEBFドライブ

バージョン: HPD3 (B) **(推奨)**
ファイル名: cp034292.compsig; cp034292.exe; cp034292.md5

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - EG0300JEHLV、EG0600JEHMA、EG0900JEHMB、およびEG1200JEHMCドライブ

バージョン: HPD5 (C) **(推奨)**
ファイル名: cp035202.compsig; cp035202.exe; cp035202.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD5を既にインストールしている場合、HPD5(C)へ更新する必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - EG0300JFCKA、EG0600JEMCV、EG0900JFCKB、およびEG1200JEMDAドライブ

バージョン: HPD6 (B) **(推奨)**

ファイル名: cp034298.compsig; cp034298.exe; cp034298.md5

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。
- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - EG1800JEHMDドライブ

バージョン: HPD6 (C) **(推奨)**
ファイル名: cp035203.compsig; cp035203.exe; cp035203.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD6を既にインストールしている場合、HPD6(C)へ更新する必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - EG1800JEMDB ドライブ

バージョン: HPD5 **(推奨)**
ファイル名: cp035863.compsig; cp035863.exe; cp035863.md5

修正

- このファームウェアには、キュー深度が小さいシーケンシャルライトワークロード時にパフォーマンスが低下する場合の修正が含まれています。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - EH000600JWCPFおよびEH000900JWCPHドライブ

バージョン: HPD4 **(推奨)**
ファイル名: cp034307.compsig; cp034307.exe; cp034307.md5

修正

- 暗号化されないFWバイナリが追加されました。
- このファームウェアには、キュー深度が小さいシーケンシャルライトワークロード時にパフォーマンスが低下する場合の修正が含まれています。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - EH0300JDYTH、EH0450JDYTK、およびEH0600JDYTL ドライブ

バージョン: HPD6 (C) **(推奨)**
ファイル名: cp035240.compsig; cp035240.exe; cp035240.md5

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります。**
- **ファームウェアバージョンHPD6を既にインストールしている場合、HPD6(C)へ更新する必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - EH0300JEDHC、EH0450JEDHD、およびEH0600JEDHEドライブ

バージョン: HPD4 (D) **(推奨)**
ファイル名: cp034316.compsig; cp034316.exe; cp034316.md5

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB010000JWAYKおよびMB008000JWAYHドライブ

バージョン: HPD5 **(クリティカル)**
ファイル名: cp036864.compsig; cp036864.exe; cp036864.md5

修正

- このコードは、アラインされていない書込みコマンドに関連する潜在的なデータの完全性の問題を修正します。これらの問題は、サプライヤーの継続的なラボテスト中でのみ検出されました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB2000JFDSLおよびMB4000JFDSNドライブ

バージョン: HPD4 (B) **(推奨)**
ファイル名: cp035643.compsig; cp035643.exe; cp035643.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**

- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD4を既にインストールしている場合、HPD4(B)へアップデートする必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB2000JFEMLおよびMB4000JFEMNドライブ

バージョン: HPD6 (B) **(クリティカル)**
ファイル名: cp035604.compsig; cp035604.exe; cp035604.md5

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**
- **ファームウェアバージョンHPD6をすでにインストールしている場合は、HPD6(B)へアップデートする必要はありません。**

修正

- プロセス中の書き込みの再試行が誤った場所で間違って開始されることによって発生する潜在的なデータ整合性の問題を修正します。 これらの問題は、サプライヤーの継続的な信頼性テスト中で検出されました。
- ファームウェアは、緊急の電源オフの改善も含まれます。

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB2000JFEPAおよびMB4000JFEPBドライブ

バージョン: HPD5 (B) **(推奨)**
ファイル名: cp035644.compsig; cp035644.exe; cp035644.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD5を既にインストールしている場合、HPD5(B)へアップデートする必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB4000JEFNCおよびMB6000JEFNDドライブ

バージョン: HPD9 (B) **(推奨)**
ファイル名: cp035638.compsig; cp035638.exe; cp035638.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD9を既にインストールしている場合、HPD9(B)へアップデートする必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB4000JEQNLおよびMB6000JEQNNドライブ

バージョン: HPDB (B) **(推奨)**
ファイル名: cp035636.compsig; cp035636.exe; cp035636.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPDBを既にインストールしている場合、HPDB(B)へ更新する必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB6000JEQUVおよびMB8000JEQVAドライブ

バージョン: HPDB (B) **(推奨)**
ファイル名: cp035648.compsig; cp035648.exe; cp035648.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPDBを既にインストールしている場合、HPDB(B)へ更新する必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB6000JVYZDおよびMB4000JVYZCドライブ

バージョン: HPD3 **(推奨)**
ファイル名: cp035592.compsig; cp035592.exe; cp035592.md5

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**

修正

- このファームウェアには、ドライブがMicrosoft Azureスタック認証の要件を満たせるようになる変更が含まれています。 さらに、特定の順次書き込み中にタイムアウトエラーが発生する可能性のあるまれなケースの問題についての修正も含まれています。

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MM1000JEFRBおよびMM2000JEFRCドライブ

バージョン: HPD8 **(オプション)**
ファイル名: cp034562.compsig; cp034562.exe; cp034562.md5

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります。**

修正

- このファームウェアにより、ドライブはAzureスタック認証の要件を満たすことができます。
- このファームウェアには、VPD 80ページに報告されているドライブシリアル番号の変更が含まれています。ドライブラベルで表示されているのと同じように報告されます。 削除されたあらゆる文字が空白のプレースホルダーに置き換えられるので、ログの形式は変わりません。

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MM1000JFJTHドライブ

バージョン: HPD3 **(オプション)**

ファイル名: cp034509.compsig; cp034509.exe; cp034509.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**

修正

- このファームウェアにより、ドライブはAzureスタック認証の要件を満たすことができます。
- このファームウェアには、VPD 80ページに報告されているドライブシリアル番号の変更が含まれています。ドライブラベルで表示されているのと同じように報告されます。 削除されたあらゆる文字が空白のプレースホルダーに置き換えられるので、ログの形式は変わりません。

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - VO1920JEUQQドライブ

バージョン: HPD3 (B) **(推奨)**
ファイル名: cp034349.compsig; cp034349.exe; cp034349.md5

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - EG000300JWBHRドライブ

バージョン: HPD3 (C) **(推奨)**
ファイル名: CP036113.compsig; CP036113.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD3を既にインストールしている場合、HPD3(C)へ更新する必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - EG0300FCSPH、EG0450FCSPK、EG0600FCSPL、およびEG0900FCSPNドライブ

バージョン: HPD2 (C) **(推奨)**
ファイル名: CP036120.compsig; CP036120.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD2を既にインストールしている場合、HPD2(C)へ更新する必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - EG0600JETKA、EG0900JETKB、およびEG1200JETKCドライブ

バージョン: HPD6 (C) **(推奨)**
ファイル名: CP036123.compsig; CP036123.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD6を既にインストールしている場合、HPD6(C)へ更新する必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - EG1800JFHMHドライブ

バージョン: HPD7 (B) **(推奨)**
ファイル名: CP036126.compsig; CP036126.zip

修正

- 暗号化されないFWバイナリが追加されました。

- このファームウェア:
  1) JetStressのREAD待ち時間パフォーマンスを改善
  2) MSAシステムで検出された内部リブートの原因を修正
  3) コントローラーが適切に処理しないベンダー固有のセンスコードを削除
  4) 潜在的なハング状態の原因を取り除くための変更が含みます

オンラインROMフラッシュコンポーネントfor VMware ESXi - EH0300JDXBA、EH0450JDXBB、およびEH0600JDXBCドライブ

バージョン: HPD5 (C) **(推奨)**
ファイル名: CP036129.compsig; CP036129.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD5を既にインストールしている場合、HPD5(C)へ更新する必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - MB1000JVYZL、MB2000JVYZN、MB3000JVYZP、およびMB4000JVYZQドライブ

バージョン: HPD2 (C) **(推奨)**
ファイル名: CP036142.compsig; CP036142.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD2を既にインストールしている場合、HPD2(C)へ更新する必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - MB6000JVYYVドライブ

バージョン: HPD2 (C) **(推奨)**
ファイル名: CP036159.compsig; CP036159.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD2を既にインストールしている場合、HPD2(C)へ更新する必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - MB8000JFECQドライブ

バージョン: HPD7 (B) **(推奨)**
ファイル名: CP036162.compsig; CP036162.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD7を既にインストールしている場合、HPD7(B)へアップデートする必要はありません。**

修正

- このファームウェアには、キュー深度が小さいシーケンシャルライトワークロード時にパフォーマンスが低下する場合の修正が含まれています。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - MO0400JFFCF、MO0800JFFCH、MO1600JFFCK、およびMO3200JFFCLドライブ

バージョン: HPD6 (B) **(推奨)**
ファイル名: CP036170.compsig; CP036170.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD6をすでにインストールしている場合は、HPD6(B)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - VO0480JFDGT、VO0960JFDGU、VO1920JFDGVおよびVO3840JFDHAドライブ

バージョン: HPD6 (C) **(推奨)**
ファイル名: CP036175.compsig; CP036175.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD6を既にインストールしている場合、HPD6(C)へ更新する必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor Windows(x64)- EG000300JWBHRドライブ

バージョン: HPD3 (B) **(推奨)**
ファイル名: cp034350.compsig; cp034350.exe; cp034350.md5

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor Windows(x64)- EG0300FCSPH、EG0450FCSPK、EG0600FCSPL、およびEG0900FCSPNドライブ

バージョン: HPD2 (B) **(推奨)**
ファイル名: cp034295.compsig; cp034295.exe; cp034295.md5

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor Windows(x64)- EG0600JETKA、EG0900JETKB、およびEG1200JETKCドライブ

バージョン: HPD6 (B) **(推奨)**
ファイル名: cp034301.compsig; cp034301.exe; cp034301.md5

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor Windows(x64)- EG1800JFHMHドライブ

バージョン: HPD7 (B) **(推奨)**
ファイル名: cp035658.compsig; cp035658.exe; cp035658.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD7を既にインストールしている場合、HPD7(B)へアップデートする必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor Windows(x64)- EH0300JDXBA、EH0450JDXBB、およびEH0600JDXBCドライブ

バージョン: HPD5 (B) **(推奨)**
ファイル名: cp034313.compsig; cp034313.exe; cp034313.md5

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor Windows(x64)- MB1000JVYZL、MB2000JVYZN、MB3000JVYZP、およびMB4000JVYZQドライブ

バージョン: HPD2 (B) **(推奨)**
ファイル名: cp035654.compsig; cp035654.exe; cp035654.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD2を既にインストールしている場合、HPD2(B)へアップデートする必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor Windows(x64)- MB6000JVYYVドライブ

バージョン: HPD2 (B) **(推奨)**
ファイル名: cp035655.compsig; cp035655.exe; cp035655.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD2を既にインストールしている場合、HPD2(B)へアップデートする必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor Windows(x64)- MB8000JFECQドライブ

バージョン: HPD7 **(推奨)**
ファイル名: cp035652.compsig; cp035652.exe; cp035652.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**

修正

- このファームウェアには、キュー深度が小さいシーケンシャルライトワークロード時にパフォーマンスが低下する場合の修正が含まれています。

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor Windows(x64)- MO0400JFFCF、MO0800JFFCH、MO1600JFFCK、およびMO3200JFFCLドライブ

バージョン: HPD6 (B) **(推奨)**
ファイル名: cp035204.compsig; cp035204.exe; cp035204.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD6をすでにインストールしている場合は、HPD6(B)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- Windows Server 2016 Device Guardのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor Windows(x64)- VO0480JFDGT、VO0960JFDGU、VO1920JFDGV、およびVO3840JFDHAドライブ

バージョン: HPD4 (D) **(推奨)**
ファイル名: cp034345.compsig; cp034345.exe; cp034345.md5

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - EG0300JEHLV、EG0600JEHMA、EG0900JEHMB、およびEG1200JEHMCドライブ

バージョン: HPD5 (C) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG5を既にインストールしている場合、HPG5(C)へ更新する必要はありません。**

拡張

- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - EG0300JFCKA、EG0600JEMCV、EG0900JFCKB、およびEG1200JEMDAドライブ

バージョン: HPD6 (C) **(推奨)**
ファイル名: 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

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) -

EG1800JEHMDドライブ

バージョン: HPD6 (C) **(推奨)**

ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD6を既にインストールしている場合、HPD6(C)へ更新する必要はありません。**

拡張

- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - EG1800JEMDBドライブ

バージョン: HPD5 (B) **(推奨)**

ファイル名: 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

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**
- **ファームウェアバージョンHPD5を既にインストールしている場合、HPD5(B)へアップデートする必要はありません。**

拡張

- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - EH0300JDYTH、EH0450JDYTK、およびEH0600JDYTL ドライブ

バージョン: HPD6 (C) **(推奨)**

ファイル名: 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

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**
- **ファームウェアバージョンHPD6を既にインストールしている場合、HPD6(C)へ更新する必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - EH0300JEDHC、EH0450JEDHD、およびEH0600JEDHEドライブ

バージョン: HPD4 (C) **(推奨)**
ファイル名: 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

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB2000JFEPAおよびMB4000JFEPBドライブ

バージョン: HPD5 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**
- **ファームウェアバージョンHPD5を既にインストールしている場合、HPD5(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB4000JEFNCおよびMB6000JEFNDドライブ

バージョン: HPD9 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**

- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**
- **ファームウェアバージョンHPD9を既にインストールしている場合、HPD9(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB4000JEQNLおよびMB6000JEQNNドライブ

バージョン: HPDB (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**
- **ファームウェアバージョンHPDBを既にインストールしている場合、HPDB(B)へ更新する必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB6000JEQUVおよびMB8000JEQVAドライブ

バージョン: HPDB (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPDBを既にインストールしている場合、HPDB(B)へ更新する必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) -

MM1000JEFRBおよびMM2000JEFRCドライブ

バージョン: HPD8 **(オプション)**

ファイル名: 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

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります。**

修正

- このファームウェアにより、ドライブはAzureスタック認証の要件を満たすことができます。
- このファームウェアには、VPD 80ページに報告されているドライブシリアル番号の変更が含まれています。ドライブラベルで表示されているのと同じように報告されます。 削除されたあらゆる文字が空白のプレースホルダーに置き換えられるので、ログの形式は変わりません。

拡張

- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MO0200JEFNV、MO0400JEFPA、MO0800JEFPB、MO1600JEFPC、EO0200JEFPD、EO0400JEFPE、およびEO0800JEFPFドライブ

バージョン: HPD3 (B) **(推奨)**

ファイル名: 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

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - VO1920JEUQQドライブ

バージョン: HPD3 (B) **(推奨)**

ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD3を既にインストールしている場合、HPD3(B) へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - EG000600JWEBHおよびEG000300JWEBFドライブ

バージョン: HPD3 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD3を既にインストールしている場合、HPD3(B) へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - EG001800JWFVCドライブ

バージョン: HPD2 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD2を既にインストールしている場合、HPD2(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - MB010000JWAYKおよびMB008000JWAYHドライブ

バージョン: HPD5 **(クリティカル)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-6ec35faf90-HPD5-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-6ec35faf90-HPD5-1.1.x86_64.rpm

修正

- このコードは、アラインされていない書込みコマンドに関連する潜在的なデータの完全性の問題を修正します。これらの問題は、サプライヤーの継続的なラボテスト中でのみ検出されました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - MB2000JFDSLおよびMB4000JFDSNドライブ

バージョン: HPD4 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**
- **ファームウェアバージョンHPD4を既にインストールしている場合、HPD4(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - MB2000JFEMLおよびMB4000JFEMNドライブ

バージョン: HPD6 (B) **(クリティカル)**
ファイル名: 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

拡張

- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - MB4000JEXYAおよびMB6000JEXYBドライブ

バージョン: HPD8 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD8を既にインストールしている場合、HPD8(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - MB6000JVYZDおよびMB4000JVYZCドライブ

バージョン: HPD3 **(推奨)**
ファイル名: 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

修正

- このファームウェアには、ドライブがMicrosoft Azureスタック認証の要件を満たせるようになる変更が含まれています。 さらに、特定の順次書き込み中にタイムアウトエラーが発生する可能性のあるまれなケースの問題についての修正も含まれています。

拡張

- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - MM1000JFJTHドライブ

バージョン: HPD3 **(オプション)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**

修正

- このファームウェアにより、ドライブはAzureスタック認証の要件を満たすことができます。
- このファームウェアには、VPD 80ページに報告されているドライブシリアル番号の変更が含まれています。ドライブラベルで表示されているのと同じように報告されます。 削除されたあらゆる文字が空白のプレースホルダーに置き換えられるので、ログの形式は変わりません。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Windows (x64) - MB4000JEXYAおよびMB6000JEXYBドライブ

バージョン: HPD8 (B) **(推奨)**
ファイル名: cp035653.compsig; cp035653.exe; cp035653.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていま**

せん。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD8を既にインストールしている場合、HPD8(B)へアップデートする必要はありません。**

拡張

- Windows Server 2016 Device Guardのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)-EG000300JWBHRドライブ

バージョン: HPD3 (C) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD3を既にインストールしている場合、HPD3(C)へ更新する必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)-EG0600JETKA、EG0900JETKB、およびEG1200JETKCドライブ

バージョン: HPD6 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD6をすでにインストールしている場合は、HPD6(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- EG1800JFHMHドライブ

バージョン: HPD7 **(推奨)**
ファイル名: 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

修正

- 暗号化されないFWバイナリが追加されました。
- このファームウェア:
  1) JetStressのREAD待ち時間パフォーマンスを改善
  2) MSAシステムで検出された内部リブートの原因を修正
  3) コントローラーが適切に処理しないベンダー固有のセンスコードを削除
  4) 潜在的なハング状態の原因を取り除くための変更が含みます

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- EH0300JDXBA、EH0450JDXBB、およびEH0600JDXBCドライブ

バージョン: HPD5 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD5を既にインストールしている場合、HPD5(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- MB1000JVYZL、MB2000JVYZN、MB3000JVYZP、およびMB4000JVYZQドライブ

バージョン: HPD2 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD2を既にインストールしている場合、HPD2(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- MB6000JVYYVドライブ

バージョン: HPD2 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPD2を既にインストールしている場合、HPD2(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- MB8000JFECQドライブ

バージョン: HPD7 **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**

修正

- このファームウェアには、キュー深度が小さいシーケンシャルライトワークロード時にパフォーマンスが低下する場合の修正が含まれています。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- MO0400JFFCF、MO0800JFFCH、MO1600JFFCK、およびMO3200JFFCLドライブ

バージョン: HPD6 (B) **(推奨)**
ファイル名: 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

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります**
- **ファームウェアバージョンHPD6をすでにインストールしている場合は、HPD6(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)-VO0480JFDGT、VO0960JFDGU、VO1920JFDGV、およびVO3840JFDHAドライブ

バージョン: HPD6 (B) **(推奨)**

ファイル名: 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

重要な注意!

- **Zero Memory(ZM)モードで動作しているSmartアレイコントローラーあるいはProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSは、Service Pack for ProLiantおよびSmart Update Managerを使用してオフラインで更新する必要があります。**
- **ファームウェアバージョンHPD6をすでにインストールしている場合は、HPD6(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。
- HPE SmartアレイP824i-p MR Gen10コントローラーのサポートを追加しました。

ファームウェア - SATAストレージディスク

先頭

Linux(x64)用サプリメンタルアップデート/オンラインROMフラッシュコンポーネント - MB001000GWCBCおよびMB002000GWCBDドライブ

バージョン: HPG4 (D) **(推奨)**

ファイル名: rpm/RPMS/x86_64/firmware-hdd-68b12e54d2-HPG4-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-68b12e54d2-HPG4-4.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**

- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(D)へアップデートする必要はありません。**

改良点:

- SLES15のサポートを追加しました。

Linux(x64)用サプリメンタルアップデート/オンラインROMフラッシュコンポーネント - MB006000GWBXQおよびMB008000GWBYLドライブ

バージョン: HPG6 (B) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-a1fd19f9ca-HPG6-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-a1fd19f9ca-HPG6-2.1.x86_64.rpm

修正

- 一部の内部診断ログ機能とレポート機能を修正しました。
- 内部バッファ管理を簡素化しました。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

Linux(x64)用サプリメンタルアップデート/オンラインROMフラッシュコンポーネント - VK0240GEPQN、VK0480GEPQP、およびVK0960GEPQQドライブ

バージョン: HPG1 (C) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-1a516522d1-HPG1-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-1a516522d1-HPG1-3.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG1を既にインストールしている場合、HPG1(C)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB001000GWFWK and MB002000GWFWLドライブ

バージョン: HPG4 (D) **(推奨)**
ファイル名: cp036261.compsig; cp036261.exe; cp036261.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB001000GWFWKおよびMB002000GWFWLドライブ

バージョン: HPG4 (D) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-bfc4af697b-HPG4-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-bfc4af697b-HPG4-4.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

VMware ESXi用オンラインROMフラッシュコンポーネント -MB006000GWBXQおよびMB008000GWBYLドライブ

バージョン: HPG5 (D) **(推奨)**
ファイル名: CP036136.compsig; CP036136.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG5を既にインストールしている場合、HPG5(D)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

Windows(x64)用オンラインROMフラッシュコンポーネント - VK0240GEPQN、VK0480GEPQP、およびVK0960GEPQQドライブ

バージョン: HPG1 (C) **(推奨)**
ファイル名: cp036286.compsig; cp036286.exe; cp036286.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていま**

せん。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG1を既にインストールしている場合、HPG1(C)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB002000GWFGHおよびMB001000GWFGFドライブ

バージョン: HPG3 (B) **(推奨)**
ファイル名: CP036135.compsig; CP036135.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG3を既にインストールしている場合、HPG3(B)へアップデートする必要はありません。**

修正

- このファームウェアには、ドライブがAzureスタック認証の要件を満たせるようになる変更が含まれています。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB010000GWAYNおよびMB008000GWAYLドライブ

バージョン: HPG5 **(クリティカル)**
ファイル名: CP036865.compsig; CP036865.zip

修正

- このコードは、アラインされていない書込みコマンドに関連する潜在的なデータの完全性の問題を修正します。これらの問題は、サプライヤーの継続的なラボテスト中でのみ検出されました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB0500GCEHF、MB1000GCEHH、およびMB2000GCEHKドライブ

バージョン: HPGD (L) **(推奨)**
ファイル名: CP036139.compsig; CP036139.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPGDを既にインストールしている場合、HPGD(L)へアップデートする必要はありません。**

修正

修正された問題点:

- HDDの長期使用後に電源の再投入後、ごくまれにデータを含むディスクの領域にドライブのヘッドが接触して、データの損失や機械的損傷を引き起こすことがあります。ファームウェア バージョンHPGDは、この状態を防ぐことができます。

HPGD (G)に対して修正された問題:

- コンポーネントが、HP ホストバスアダプター H22xへ取り付けられている2つ以上の外部ドライブエンクロージャーで構成されるシステム内に含まれるドライブのドライブファームウェアのインストールに失敗しました。「ドライブがツリー内に数回表示されています」というメッセージがコンポーネントログファイルに報告されました。ドライブファームウェアインストールの失敗は、HPホストバスアダプター H22xへ取り付けられている1つの外部ドライブエンクロージャーがある構成内では観察されませんでした。

HPGD (J)に対して修正された問題:

- VMware vSphere 6.5環境でドライブファームウェアをアップデートしようとすると、アップデートに失敗し、イベントがセグメント障害エラーとして記録されます。

拡張

改善点/新しい機能:

- VMware vSphere 5.5のサポートを追加。
- UEFI(Universal Extensible Firmware Interface)ベースのサーバーのサポートを追加しました。
- HP Dynamic SmartアレイB140iコントローラーに関するサポートを追加しました。

HPGD (F)の改善点/新しい機能:

- すべてのSATAドライブコンポーネント全体でログを標準化するようにフラッシュエンジンを更新しました。
- コンポーネントログファイルで提供される詳細を改善するためにログ機能を拡張しました。
- VMwareファームウェアSmartコンポーネントパッケージは*.scexeパッケージから *.zip パッケージに変更され、インストール中の改良されたセキュリティを提供する実行可能なバイナリを含んでいます。VMware Smartコンポーネントの機能に変更はありません。

HPGD (H)の改善された/新しい機能:

- VMware vSphere 6.5のサポートを追加します。

HPGD (K)の改善点/新しい機能:

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB1000GCWCV、MB2000GCWDA、MB3000GCWDB および MB4000GCWDCドライブ

バージョン: HPGI (D) **(推奨)**
ファイル名: CP036112.compsig; CP036112.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを**

使用したオフライン更新が必要です。
- **ファームウェアバージョンHPGIを既にインストールしている場合、HPGI(D)へアップデートする必要はありません。**

修正

- このファームウェアは、ホストが100ミリ秒の非アクティブ状態になった後、ランダムシークを実行する機能を実装します。

拡張

改善点/新しい機能:

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB2000GCVBR、MB3000GCVBT、およびMB4000GCVBUドライブ

バージョン: HPG5 (H) **(推奨)**
ファイル名: CP036143.compsig; CP036143.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG5を既にインストールしている場合、HPG5(H)へ更新する必要はありません。**

修正

修正された問題点:

- データが誤ったセクターに書かれる可能性があった、低い5v駆動電圧と特定の順次データストリーミング状態の間のまれではあるが潜在的なデータ整合性エラーを修正します。

HPG5 (C)に対して修正された問題:

- コンポーネントが、HP ホストバスアダプター H22xへ取り付けられている2つ以上の外部ドライブエンクロージャーで構成されるシステム内に含まれるドライブのドライブファームウェアのインストールに失敗しました。「ドライブがツリー内に数回表示されています」というメッセージがコンポーネントログファイルに報告されました。ドライブファームウェアインストールの失敗は、HPホストバスアダプター H22xへ取り付けられている1つの外部ドライブエンクロージャーがある構成内では観察されませんでした。

HPG5 (E)に対して修正された問題:

- VMware vSphere 6.5環境でドライブファームウェアをアップデートしようとすると、アップデートに失敗し、イベントがセグメント障害エラーとして記録されます。

拡張

HPG5 (B)の改善点/新しい機能:

- すべてのSATAドライブコンポーネント全体でログを標準化するようにフラッシュエンジンを更新しました。
- コンポーネントログファイルで提供される詳細を改善するためにログ機能を拡張しました。
- VMwareファームウェアSmartコンポーネントパッケージは*.scexeパッケージから *.zip パッケージに変更され、インストール中の改良されたセキュリティを提供する実行可能なバイナリを含んでいます。VMware Smartコンポーネント

の機能に変更はありません。

HPG5 (D)の改善点/新しい機能:

- VMware vSphere 6.5のサポートを追加します。

HPGD (K)の改善点/新しい機能:

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB2000GCWLT, MB3000GCWLUおよびMB4000GCWLVドライブ

バージョン: HPG4 (E) **(推奨)**
ファイル名: CP036144.compsig; CP036144.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(E)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB2000GFEMHおよびMB4000GFEMKドライブ

バージョン: HPG6 (C) **(クリティカル)**
ファイル名: CP036145.compsig; CP036145.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG6を既にインストールしている場合、HPG6(C)へアップデートする必要はありません。**

修正

- プロセス中の書き込みの再試行が誤った場所で間違って開始されることによって発生する潜在的なデータ整合性の問題を修正します。 これらの問題は、サプライヤーの継続的な信頼性テスト中で検出されました。

- ファームウェアは、コードのダウンロード後に設定の保存を修正し、緊急電源オフの改善を含みます。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB4000GEQNHおよびMB6000GEQNKドライブ

バージョン: HPGB (C) **(推奨)**
ファイル名: CP036150.compsig; CP036150.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPGBを既にインストールしている場合、HPGB(C)へアップデートする必要はありません。**

修正

- プロセス中の書き込みの再試行が誤った場所で間違って開始されることによって発生する潜在的なデータ整合性の問題を修正します。 これらの問題は、サプライヤーの継続的な信頼性テスト中で検出されました。
- ファームウェアは、コードのダウンロード後に設定の保存を修正し、緊急電源オフの改善を含みます。

拡張

HPGB (B)の改善点/新しい機能:

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MB6000GEQUTおよびMB8000GEQUUドライブ

バージョン: HPGB (C) **(クリティカル)**
ファイル名: CP036155.compsig; CP036155.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPGBを既にインストールしている場合、HPGB(C)へアップデートする必要はありません。**

修正

- プロセス中の書き込みの再試行が誤った場所で間違って開始されることによって発生する潜在的なデータ整合性の問題を修正します。 これらの問題は、サプライヤーの継続的な信頼性テスト中でのみ検出されました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MK0960GECQKドライブ

バージョン: HPG3 (F) **(推奨)**
ファイル名: CP036164.compsig; CP036164.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG3を既にインストールしている場合、HPG3(F)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MM1000GEFQVおよびMM2000GEFRAドライブ

バージョン: HPG5 (D) **(推奨)**
ファイル名: CP036165.compsig; CP036165.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG5を既にインストールしている場合、HPG5(D)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - MM1000GFJTEドライブ

バージョン: HPG1 (E) **(推奨)**
ファイル名: CP036166.compsig; CP036166.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG1を既にインストールしている場合、HPG1(E)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB010000GWAYNおよびMB008000GWAYLドライブ

バージョン: HPG5 **(クリティカル)**
ファイル名: cp036866.compsig; cp036866.exe; cp036866.md5

修正

- このコードは、アラインされていない書込みコマンドに関連する潜在的なデータの完全性の問題を修正します。これらの問題は、サプライヤーの継続的なラボテスト中でのみ検出されました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB0500GCEHF、MB1000GCEHH、およびMB2000GCEHKドライブ

バージョン: HPGD (G) **(推奨)**
ファイル名: cp036265.compsig; cp036265.exe; cp036265.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPGDを既にインストールしている場合、HPGD(G)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB1000GCWCV、MB2000GCWDA、MB3000GCWDB および MB4000GCWDCドライブ

バージョン: HPGI (C) **(推奨)**
ファイル名: cp036266.compsig; cp036266.exe; cp036266.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPGIを既にインストールしている場合、HPGI(C)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB1000GDUNU, MB2000GDUNV, MB3000GDUPA, およびMB4000GDUPBドライブ

バージョン: HPG4 (D) **(推奨)**
ファイル名: cp036267.compsig; cp036267.exe; cp036267.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB2000GCVBR、MB3000GCVBT、およびMB4000GCVBUドライブ

バージョン: HPG5 (F) **(推奨)**
ファイル名: cp036269.compsig; cp036269.exe; cp036269.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG5を既にインストールしている場合、HPG5(F)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB2000GFEMHおよびMB4000GFEMKドライブ

バージョン: HPG6 (C) **(クリティカル)**
ファイル名: cp036271.compsig; cp036271.exe; cp036271.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG6を既にインストールしている場合、HPG6(C)へアップデートする必要はありません。**

修正

- プロセス中の書き込みの再試行が誤った場所で間違って開始されることによって発生する潜在的なデータ整合性の問題を修正します。 これらの問題は、サプライヤーの継続的な信頼性テスト中で検出されました。

- ファームウェアは、コードのダウンロード後に設定の保存を修正し、緊急電源オフの改善を含みます。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB4000GEFNAおよびMB6000GEFNBドライブ

バージョン: HPG6 (D) **(推奨)**
ファイル名: cp036272.compsig; cp036272.exe; cp036272.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG6を既にインストールしている場合、HPG6(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB4000GEQNHおよびMB6000GEQNKドライブ

バージョン: HPGB (C) **(推奨)**
ファイル名: cp036273.compsig; cp036273.exe; cp036273.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPGBを既にインストールしている場合、HPGB(C)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネント for Windows (x64) - MB6000GEQUTおよびMB8000GEQUUドライブ

バージョン: HPGB (C) **(クリティカル)**
ファイル名: cp036275.compsig; cp036275.exe; cp036275.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPGBを既にインストールしている場合、HPGB(C)へアップデートする必要はありません。**

修正

- プロセス中の書き込みの再試行が誤った場所で間違って開始されることによって発生する潜在的なデータ整合性の問題を修正します。 これらの問題は、サプライヤーの継続的な信頼性テスト中でのみ検出されました。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネント for Windows (x64) - MK0960GECQKドライブ

バージョン: HPG3 (F) **(推奨)**
ファイル名: cp036280.compsig; cp036280.exe; cp036280.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG3を既にインストールしている場合、HPG3(F)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネント for Windows (x64) - MM1000GEFQVおよびMM2000GEFRAドライブ

バージョン: HPG8 (B) **(推奨)**
ファイル名: cp036834.compsig; cp036834.exe; cp036834.md5

修正

- このファームウェアは、NDUコンプライアンスを示すようにドライブをアップデートします。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

オンラインROMフラッシュコンポーネント for Windows (x64) - MM1000GFJTEドライブ

バージョン: HPG4 (B) **(推奨)**
ファイル名: cp036835.compsig; cp036835.exe; cp036835.md5

修正

- このファームウェアは、NDUコンプライアンスを示すようにドライブをアップデートします。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネントfor VMware ESXi - MB1000GVYZE、MB2000GVYZF、MB3000GVYZH、およびMB4000GVYZKドライブ

バージョン: HPG4 (C) **(推奨)**
ファイル名: CP036141.compsig; CP036141.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**

- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(C)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - MB6000GVYYUドライブ

バージョン: HPG2 (C) **(推奨)**
ファイル名: CP036157.compsig; CP036157.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG2を既にインストールしている場合、HPG2(C)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - XP0032GEFEN、XP0032GDZME、XP0064GEFEP、およびXP0064GDZMFドライブ

バージョン: HPS8 (D) **(推奨)**
ファイル名: CP036177.compsig; CP036177.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPS8を既にインストールしている場合、HPS8(D)へアップデートする必要はありません。**

事前要件

ドライブモデルXP0032GEFEN、XP0032GDZME、XP0064GDZMF、およびXP0064GEFEPでは、ファームウェアバージョンHPS8にアップデートする前に、ファームウェアバージョンHPS6がインストールされていることが必要です。

修正

ファームウェアの関連性:

- ドライブモデルXP0032GEFEN、XP0032GDZME、XP0064GDZMF、およびXP0064GEFEPでは、ファームウェアバージョンHPS8にアップデートする前に、ファームウェアバージョンHPS6がインストールされていることが必要です。

修正された問題点:

- HPS8 のファームウェアリリースは、ドライブの長いセルフテスト中にドライブがシステムにより認識されなくするタイムアウト状態を起こすというファームウェアのタイミングの問題を解決しました。

HPS8 (B)に対して修正された問題:

- VMware vSphere 6.5環境でドライブファームウェアをアップデートしようとすると、アップデートに失敗し、イベントがセグメント障害エラーとして記録されます。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - XP0120GFJSLおよびXP0240GFJSNドライブ

バージョン: HPS4 (D) **(推奨)**
ファイル名: CP036178.compsig; CP036178.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPS4を既にインストールしている場合、HPS4(D)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

オンラインROMフラッシュコンポーネントfor Windows (x64) - VK0120GFDKE、VK0240GFDKF、VK0480GFDKH、VK0960GFDKK、VK1920GFDKL、およびVK3840GFDKNドライブ

バージョン: HPG1 (C) **(推奨)**
ファイル名: cp036285.compsig; cp036285.exe; cp036285.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG1を既にインストールしている場合、HPG1(C)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネントfor Windows (x64) - XP0032GEFEN、XP0032GDZME、XP0064GEFEP、およびXP0064GDZMFドライブ

バージョン: HPS8 (C) **(推奨)**

ファイル名: cp036287.compsig; cp036287.exe; cp036287.md5

事前要件

ドライブモデルXP0032GEFEN、XP0032GDZME、XP0064GDZMF、およびXP0064GEFEPでは、ファームウェアバージョンHPS8にアップデートする前に、ファームウェアバージョンHPS6がインストールされていることが必要です。

オンラインROMフラッシュコンポーネントfor Windows (x64) - XP0120GFJSLおよびXP0240GFJSNドライブ

バージョン: HPS4 (C) **(推奨)**
ファイル名: cp036288.compsig; cp036288.exe; cp036288.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPS4を既にインストールしている場合、HPS4(C)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネントfor Windows(x64)- MB1000GVYZE、MB2000GVYZF、MB3000GVYZH、およびMB4000GVYZKドライブ

バージョン: HPG4 (D) **(推奨)**
ファイル名: cp036268.compsig; cp036268.exe; cp036268.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネントfor Windows(x64)- MB2000GCWLT、MB3000GCWLU、およびMB4000GCWLVドライブ

バージョン: HPG4 (D) **(推奨)**
ファイル名: cp036270.compsig; cp036270.exe; cp036270.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていま**

せん。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネントfor Windows(x64)- MB6000GEBTPドライブ

バージョン: HPG4 (C) **(推奨)**
ファイル名: cp036274.compsig; cp036274.exe; cp036274.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(C)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネントfor Windows(x64)- MB6000GEXXVドライブ

バージョン: HPG2 (D) **(推奨)**
ファイル名: cp036276.compsig; cp036276.exe; cp036276.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG2を既にインストールしている場合、HPG2(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネントfor Windows(x64)- MB6000GVYYUドライブ

バージョン: HPG2 (C) **(推奨)**
ファイル名: cp036277.compsig; cp036277.exe; cp036277.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていま**

せん。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG2を既にインストールしている場合、HPG2(C)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

オンラインROMフラッシュコンポーネントfor Windows(x64)- MB8000GFECRドライブ

バージョン: HPG5 (C) **(推奨)**
ファイル名: cp036278.compsig; cp036278.exe; cp036278.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG5を既にインストールしている場合、HPG5(C)へ更新する必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for ESXi - MB1000GDUNU, MB2000GDUNV, MB3000GDUPA, およびMB4000GDUPBドライブ

バージョン: HPG4 (E) **(推奨)**
ファイル名: CP036140.compsig; CP036140.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(E)へアップデートする必要はありません。**

修正

修正された問題点:

- トラックの狭い範囲にデータを書き込むアプリケーションの信頼性の向上。

HPG4 (C)に対して修正された問題:

- VMware vSphere 6.5環境でドライブファームウェアをアップデートしようとすると、アップデートに失敗し、イベントがセグメント障害エラーとして記録されます。

既知の問題点:

- ファームウェアは、HPG4へのアップグレード後、HPG3へダウングレードすることはできません。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB2000GCVBR、MB3000GCVBT、およびMB4000GCVBUドライブ

バージョン: HPG5 (E) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-e4f5b5c9a7-HPG5-5.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-e4f5b5c9a7-HPG5-5.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーに接続されているドライブへオンラインでファームウェア (ZM) モードまたは HPE ProLiant ホスト バス アダプター (HBA) はサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG5を既にインストールしている場合、HPG5(E)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB0500GCEHF、MB1000GCEHH、およびMB2000GCEHKドライブ

バージョン: HPGD (G) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-b583d96f94-HPGD-7.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-b583d96f94-HPGD-7.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE SmartアレイコントローラーあるいはHPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPGDを既にインストールしている場合、HPGD(G)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB1000GCWCV、MB2000GCWDA、MB3000GCWDB および MB4000GCWDCドライブ

バージョン: HPGI (D) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-a1b08f8a6b-HPGI-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-a1b08f8a6b-HPGI-4.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPGIを既にインストールしている場合、HPGI(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB1000GDUNU, MB2000GDUNV, MB3000GDUPA, およびMB4000GDUPBドライブ

バージョン: HPG4 (D) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-3ab4c70e64-HPG4-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-3ab4c70e64-HPG4-4.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB4000GEFNAおよびMB6000GEFNBドライブ

バージョン: HPG6 (D) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-40277d55d3-HPG6-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-40277d55d3-HPG6-4.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG6を既にインストールしている場合、HPG6(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB4000GEQNHおよびMB6000GEQNKドライブ

バージョン: HPGB (C) **(クリティカル)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-bfc95f0628-HPGB-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-bfc95f0628-HPGB-3.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPGBを既にインストールしている場合、HPGB(C)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。
- プロセス中の書き込みの再試行が誤った場所で間違って開始されることによって発生する潜在的なデータ整合性の問題を修正します。 これらの問題は、サプライヤーの継続的なラボテスト中でのみ検出されました。
- ファームウェアは、コードのダウンロード後に設定の保存を修正し、緊急電源オフの改善を含みます。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB6000GEBTPドライブ

バージョン: HPG4 (C) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-3243fce9a0-HPG4-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-3243fce9a0-HPG4-3.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(C)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MB6000GEQUTおよびMB8000GEQUUドライブ

バージョン: HPGB (C) **(クリティカル)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-1d7f19120b-HPGB-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-

1d7f19120b-HPGB-3.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPGBを既にインストールしている場合、HPGB(C)へアップデートする必要はありません。**

修正

- プロセス中の書き込みの再試行が誤った場所で間違って開始されることによって発生する潜在的なデータ整合性の問題を修正します。 これらの問題は、サプライヤーの継続的な信頼性テスト中でのみ検出されました。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MK0960GECQKドライブ

バージョン: HPG3 (E) **(クリティカル)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-3e34285be7-HPG3-5.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-3e34285be7-HPG3-5.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG3を既にインストールしている場合、HPG3(E)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。
- ファームウェアは、非整列シーケンシャル書き込み操作に関連する断続的なデータの破損問題を修正します。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - MM1000GEFQVおよびMM2000GEFRAドライブ

バージョン: HPG8 (B) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-ec908c3650-HPG8-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-ec908c3650-HPG8-2.1.x86_64.rpm

修正

- このファームウェアは、NDUコンプライアンスを示すようにドライブをアップデートします。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) -

MM1000GFJTEドライブ

バージョン: HPG4 (B) **(推奨)**

ファイル名: rpm/RPMS/x86_64/firmware-hdd-95af9a555e-HPG4-2.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-95af9a555e-HPG4-2.1.x86_64.rpm

修正

- このファームウェアは、NDUコンプライアンスを示すようにドライブをアップデートします。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネントfor Linux (x64) - XP0032GEFEN、XP0032GDZME、XP0064GEFEP、およびXP0064GDZMFドライブ

バージョン: HPS8 (D) **(推奨)**

ファイル名: rpm/RPMS/x86_64/firmware-hdd-f286f98973-HPS8-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-f286f98973-HPS8-4.1.x86_64.rpm

事前要件

ドライブモデルXP0032GEFEN、XP0032GDZME、XP0064GDZMF、およびXP0064GEFEPでは、ファームウェアバージョンHPS8にアップデートする前に、ファームウェアバージョンHPS5がインストールされていることが必要です。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネントfor Linux (x64) - XP0120GFJSLおよびXP0240GFJSN ドライブ

バージョン: HPS4 (D) **(推奨)**

ファイル名: rpm/RPMS/x86_64/firmware-hdd-d355375539-HPS4-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-d355375539-HPS4-4.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPS4を既にインストールしている場合、HPS4(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for ESXi - MB001000GWCBCおよびMB002000GWCBDドライブ

バージョン: HPG4 (C) **(推奨)**

ファイル名: CP036133.compsig; CP036133.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを**

使用したオフライン更新が必要です。
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(C)へアップデートする必要はありません。**

修正

修正された問題点:

- このファームウェアは、保管した追跡のデータが適切にアップデートされていない潜在的問題を作り、ドライブが電源を入れるときのブートプロセスを終了させない危険を消去します。
- その他のメンテナンスの修正とアップデートは、新しいファームウェアに含まれています。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for ESXi - MB001000GWCBCおよびMB002000GWCBDドライブ

バージョン: HPG4 (C) **(推奨)**
ファイル名: CP036134.compsig; CP036134.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(C)へアップデートする必要はありません。**

拡張

- ファームウェアバージョンHGP4は、ドライブがHPG4ファームウェアにアップデートした後、ファームウェアの以前のバージョンがドライブにロードされることを防ぐように設定されています。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for ESXi - MB4000GEFNAおよびMB6000GEFNBドライブ

バージョン: HPG6 (C) **(推奨)**
ファイル名: CP036149.compsig; CP036149.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG6を既にインストールしている場合、HPG6(C)へアップデートする必要はありません。**

修正

修正された問題点:

- HPG6ファームウェアは、ディスクドライブが1秒を超える長時間のホスト非アクティビティ状態に陥ったときに、ドライブの信頼性を改善します。

拡張

HPG6(B)の改善点/新しい機能:

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for ESXi - MB6000GEBTPドライブ

バージョン: HPG4 (C) **(推奨)**
ファイル名: CP036154.compsig; CP036154.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(C)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for ESXi - MB6000GEXXVドライブ

バージョン: HPG2 (E) **(推奨)**
ファイル名: CP036156.compsig; CP036156.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG2を既にインストールしている場合、HPG2(E)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for ESXi - MB8000GFECRドライブ

バージョン: HPG5 (B) **(推奨)**
ファイル名: CP036161.compsig; CP036161.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG5を既にインストールしている場合、HPG5(B)へアップデートする必要はありません。**

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for ESXi - VK0240GEPQN、VK0480GEPQP、およびVK0960GEPQQドライブ

バージョン: HPG1 (D) **(推奨)**
ファイル名: CP036174.compsig; CP036174.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG1を既にインストールしている場合、HPG1(D)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - MB010000GWAYNおよびMB008000GWAYLドライブ

バージョン: HPG5 **(クリティカル)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-cc819d4bff-HPG5-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-cc819d4bff-HPG5-1.1.x86_64.rpm

修正

- このコードは、アライメントされていない書き込みコマンドに関連する潜在的なデータ整合性の問題を修正します。このサプライヤーの継続的なラボ テストで発見されました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - MB2000GFEMHおよびMB4000GFEMKドライブ

バージョン: HPG6 (C) **(クリティカル)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-70e3962f98-HPG6-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-70e3962f98-HPG6-3.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG6を既にインストールしている場合、HPG6(C)へアップデートする必要はありません。**

修正

- プロセス中の書き込みの再試行が誤った場所で間違って開始されることによって発生する潜在的なデータ整合性の問題を修正します。 これらの問題は、サプライヤーの継続的な信頼性テスト中で検出されました。
- ファームウェアは、コードのダウンロード後に設定の保存を修正し、緊急電源オフの改善を含みます。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Windows (x64) - MB001000GWCBCおよびMB002000GWCBDドライブ

バージョン: HPG4 (D) **(推奨)**
ファイル名: cp036260.compsig; cp036260.exe; cp036260.md5

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Windows (x64) - MB006000GWBXQおよびMB008000GWBYLドライブ

バージョン: HPG6 (B) **(推奨)**
ファイル名: cp036838.compsig; cp036838.exe; cp036838.md5

修正

- 一部の内部診断ログ機能とレポート機能を修正しました。
- 内部バッファ管理を簡素化しました。
- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗します。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor ESXi - VK0120GFDKE、VK0240GFDKF、VK0480GFDKH、VK0960GFDKK、VK1920GFDKL、およびVK3840GFDKNドライブ

バージョン: HPG1 (D) **(推奨)**
ファイル名: CP036173.compsig; CP036173.zip

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG1を既にインストールしている場合、HPG1(D)へアップデートする必要はありません。**

修正

- 暗号化されないFWバイナリが追加されました。

拡張

- SmartRAID 3154-8e RAIDコントローラーのサポートを追加しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux (x64) - VK0120GFDKE、VK0240GFDKF、VK0480GFDKH、VK0960GFDKK、VK1920GFDKL、および VK3840GFDKNドライブ

バージョン: HPG1 (D) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-a2d4b5c742-HPG1-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-a2d4b5c742-HPG1-4.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG1を既にインストールしている場合、HPG1(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- MB1000GVYZE、MB2000GVYZF、MB3000GVYZH、およびMB4000GVYZKドライブ

バージョン: HPG4 (D) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-0a7010918e-HPG4-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-0a7010918e-HPG4-4.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを**

使用したオフライン更新が必要です。
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- MB2000GCWLT、MB3000GCWLU、およびMB4000GCWLVドライブ

バージョン: HPG4 (D) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-2e70ce7412-HPG4-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-2e70ce7412-HPG4-4.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG4を既にインストールしている場合、HPG4(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- MB6000GEXXVドライブ

バージョン: HPG2 (D) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-a629fcea59-HPG2-4.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-a629fcea59-HPG2-4.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG2を既にインストールしている場合、HPG2(D)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- MB6000GVYYUドライブ

バージョン: HPG2 (C) **(推奨)**

ファイル名: rpm/RPMS/x86_64/firmware-hdd-bdc37cb37f-HPG2-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-bdc37cb37f-HPG2-3.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG2を既にインストールしている場合、HPG2(C)へアップデートする必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネントfor Linux(x64)- MB8000GFECR ドライブ

バージョン: HPG5 (C) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-hdd-6d922fc9a8-HPG5-3.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-hdd-6d922fc9a8-HPG5-3.1.x86_64.rpm

重要な注意!

- **Zero Memory (ZM) モードで動作しているHPE Smartアレイコントローラーあるいは HPE ProLiantのホストバスアダプター(HBA)に接続されているドライブへオンラインでファームウェアをフラッシュすることはサポートされていません。これらの構成では、ドライブへオフラインでファームウェアをフラッシュすることだけがサポートされています。**
- **サポートされるLinux、Microsoft WindowsおよびVMware環境を実行しているシステムで構成されたSmartアレイコントローラーで利用可能なオンラインドライブファームウェアの更新。他のすべてのOSでは、SPPおよびHP SUMを使用したオフライン更新が必要です。**
- **ファームウェアバージョンHPG5を既にインストールしている場合、HPG5(C)へ更新する必要はありません。**

修正

- ドライブがAHCIコントローラーの背後で接続されているときにオンラインファームウェアアップデートが失敗するという問題を修正しました。

ファームウェア - ストレージコントローラー

先頭

Online ROM Flash Component for ESXi (x86) - HPE Smartアレイ P824i-p MR Gen10

バージョン: 24.23.0-0019 (B) **(オプション)**
ファイル名: CP035399.compsig; CP035399.zip

重要な注意!

すでにファームウェアバージョン24.23.0-0019をインストールしている場合、24.23.0-0019(B)にアップデートする必要はありません。

拡張

- Smart Update Managerとの統合を強化しました。

オンラインROMフラッシュコンポーネント for Linux (x64) - HPE Smartアレイ P824i-p MR Gen10

バージョン: 24.23.0-0019 **(オプション)**
ファイル名: 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

拡張

- 最初のリリース

VMware ESXi用オンラインROMフラッシュコンポーネント - HPE SmartアレイP408i-p、P408e-p、P408i-a、P408i-c、E208i-p、E208e-p、E208i-c、E208i-a、P204i-c、P204i-b、P816i-a、およびP416ie-m SR Gen10

バージョン: 1.65 **(推奨)**
ファイル名: CP037352.compsig; CP037352.zip

修正

- システムがPOST中に応答しなくなり、OSのロードに失敗することがありました。この問題は、システム BIOSのバージョンが1.40以降の場合に発生する可能性が高くなります。ただし、以前のBIOSバージョンを実行しているシステムでもこの問題が発生する可能性があります。

Windows(x64)用オンラインROMフラッシュコンポーネント - HPE SmartアレイP408i-p、P408e-p、P408i-a、P408i-c、E208i-p、E208e-p、E208i-c、E208i-a、P204i-c、P204i-b、P816i-a、およびP416ie-m SR Gen10

バージョン: 1.65 **(推奨)**
ファイル名: cp037353.compsig; cp037353.exe; cp037353.md5

修正

- システムがPOST中に応答しなくなり、OSのロードに失敗することがありました。この問題は、システム BIOSのバージョンが1.40以降の場合に発生する可能性が高くなります。ただし、以前のBIOSバージョンを実行しているシステムでもこの問題が発生する可能性があります。

オンラインROM Flashコンポーネント for Windows (x64) - HPE SmartアレイP824i-p MR Gen10

バージョン: 24.23.0-0019 (B) **(オプション)**
ファイル名: cp035040.compsig; cp035040.exe; cp035040.md5

重要な注意!

- すでにファームウェアバージョン24.23.0-0019をインストールしている場合、24.23.0-0019(B)にアップデートする必要はありません。

拡張

- HPEデジタル署名を追加しました

オンラインROMフラッシュコンポーネント for Linux - HPEホストバスアダプターH221

バージョン: 15.10.10.00 (B) **(オプション)**
ファイル名: rpm/RPMS/i386/firmware-43d7eff89e-15.10.10.00-2.1.i386.rpm

重要な注意！

このドライバーコンポーネントは、H221コントローラー搭載のGen9サーバーのみをサポートし、コントローラーはGen9サーバーでのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしません。

修正

Service Pack ProLiant(SPP)を使用するときに、ホストバスアダプター(HBA)Stockade(H2xx)ドライバーの適切なFWバージョンがインストールされない問題を修正しました

サポートしているデバイスおよび機能

このドライバーコンポーネントは、H221コントローラー搭載のGen9サーバーのみをサポートし、コントローラーはGen9サーバーでのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしません。

オンラインROMフラッシュコンポーネント for Linux (x64) - HPE Apollo 2000 System - SASエキスパンダー

バージョン: 1.00 (B) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-smartarray-3bf7ece88e-1.00-2.1.x86_64.rpm

重要な注意!

- ファームウェアバージョン1.00を既にインストールしている場合、1.00 (B)へアップデートする必要はありません。

拡張

- Smart Update Managerとの統合を強化しました。

  注記:Apollo 2000 SAS Expanderが以前にバージョン1.00にアップデートされている場合、バージョン1.00(B)にアップグレードする必要はありません。

オンラインROMフラッシュコンポーネント for Linux(x64) - HPE Apollo 2000 Gen10バックプレーンエキスパンダーファームウェア

バージョン: 1.00 **(オプション)**
ファイル名: 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

拡張

最初のリリース

オンラインROMフラッシュコンポーネント for VMware ESXi - HPE Apollo 2000 System - SASエキスパンダー

バージョン: 1.00 (B) **(推奨)**
ファイル名: CP031314.compsig; CP031314.zip

重要な注意!

- **ファームウェアバージョン1.00を既にインストールしている場合、1.00 (B)へアップデートする必要はありません。**

拡張

- VMware vSphere 2016 OSのサポートを追加しました。
- Smart Update Managerとの統合を強化しました。
  注記:Apollo 2000 SAS Expanderが以前にバージョン1.00にアップデートされている場合、バージョン1.00(B)にアッ

プグレードする必要はありません。

オンラインROMフラッシュコンポーネント for VMware ESXi - HPE 12 Gb/s SASエキスパンダーファームウェア for HPE Smartアレイコントローラーおよび HPE HBAコントローラー

バージョン: 4.02 **(オプション)**
ファイル名: CP033904.compsig; CP033904.zip

重要な注意！

- ファームウェアがバージョン1.31またはそれ以前からアップグレードされた場合には、電源再投入/コールドリブートが必要です。

修正

- 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.

オンラインROMフラッシュコンポーネント for VMware ESXi - HPE Apollo 4200 Gen9バックプレーンエキスパンダーファームウェア

バージョン: 1.50 (B) **(オプション)**
ファイル名: CP036095.zip

重要な注意！

- ファームウェアがバージョン1.03またはそれ以前からアップグレードされた場合には、電源再投入/コールドリブートが必要です。

オンラインROMフラッシュコンポーネント for VMware ESXi - HPE Express Bay Enablement Switch カード

バージョン: 1.78 **(オプション)**
ファイル名: CP033861.zip

重要な注意！

- アップデートを有効にするには、インストール後に電源再投入/コールドリブートが必要です。

事前要件

- HP ProLiant iLOファームウェアバージョンは、v2.20以降である必要があります。 HP ProLiant iLOファームウェアがv2.20より古い場合、以下のエラーメッセージを受け取ります。

  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

修正

Seagate NVMeハードドライブの温度ステータスを修正しました。

オンラインROMフラッシュコンポーネント for VMware ESXi - HPEデュアル 8GB MicroSD USB

バージョン: 1.3.2.215 **(推奨)**
ファイル名: CP034825.compsig; CP034825.zip

修正

- Agentless Management Serviceバージョン11.2.0以降で、対応するHPEデュアル8GB Micron SDパーツ番号を表示します。

オンラインROMフラッシュコンポーネント for VMware ESXi - Smartアレイ H240ar、H240、H240nr、H241、H244br、P240nr、P244br、P246br、P440ar、P440、P441、P542D、P741m、P840、P840arおよびP841

バージョン: 6.60 **(推奨)**
ファイル名: CP035732.compsig; CP035732.zip

修正

- QueryAsynchronousEventが不適切な応答データを提供する可能性がある問題
- 数回の再起動後にキャッシュが無効になる可能性があるという問題

拡張

- 大きな容量サイズのスマートキャッシュに対するサポートが追加されました

オンラインROMフラッシュコンポーネント for VMware ESXi - SmartアレイP220i、P222、P420i、P420、P421、P721m、およびP822

バージョン: 8.32 **(推奨)**
ファイル名: CP033366.compsig; CP033366.zip

修正

システムは、ベースコードファームウェアによって返される完了について、RAIDスタックスレッドがキューをポーリングしているライブロック状況のために、ロックアップコードを表示せずに応答を停止することがあります。

拡張

ドライブ温度レポート機能の精度が改善されました。

オンラインROMフラッシュコンポーネント for VMware ESXi - SmartアレイP230i、P430、P431、P731m、P830i および P830

バージョン: 4.54 (B) **(推奨)**
ファイル名: CP036098.compsig; CP036098.zip

修正

- DDRキャッシュは数回起動した後に、ランダムに無効になります。
- 元のドライブが障害予測を持つと特定された場合、hot-inserted交換ドライブは、障害予測として表示される可能性があります。
- コントローラーキャッシュモジュールは、Smartストレージバッテリが取り外されているかシステムがオンラインの時に障害が発生すると、バックアップ電源なしでの書き込みキャッシングの有効化に以前はSSAが使用されていたとしても、永久的に無効としてマークが付けられる可能性があります。

- 先読みと読み取り入力が順番に実行されるときにスマートキャッシュがフラッシュ操作を保留中であるため、コントローラーが応答しなくなることがあります。
- RAID6ボリュームのサーフェース・スキャン中にパリティエラーが見つかった場合、システムが応答を停止することがあります。(POST Lockup 0x13)
- 接続されたドライブがスピンダウンされた場合は、システムファンが100%に到達する可能性があります
- コントローラーの障害が発生した後で、コントローラークラッシュダンプが収集されない可能性がある問題

オンラインROMフラッシュコンポーネント for Windows (x64) - HP Apollo 4200 Gen9バックプレーンエキスパンダーファームウェア

バージョン: 1.50 (B) **(オプション)**
ファイル名: rpm/RPMS/x86_64/firmware-smartarray-f18fdefd0b-1.50-2.1.x86_64.rpm

重要な注意！

- ファームウェアがバージョン1.03またはそれ以前からアップグレードされた場合には、電源再投入/コールドリブートが必要です。

オンラインROMフラッシュコンポーネント for Windows (x64) - HPE 12Gb/s SASエキスパンダーファームウェア for HPE Smartアレイコントローラーおよび HPE HBAコントローラー

バージョン: 4.02 (B) **(オプション)**
ファイル名: cp034755.compsig; cp034755.exe; cp034755.md5

重要な注意！

- すでにファームウェアバージョン4.02をインストールしている場合、4.02 (B)にアップデートする必要はありません。
- ファームウェアがバージョン1.31またはそれ以前からアップグレードされた場合には、電源再投入/コールドリブートが必要です。

オンラインROMフラッシュコンポーネント for Windows (x64) - HPE Apollo 2000 Gen10バックプレーンエキスパンダーファームウェア

バージョン: 1.00 **(オプション)**
ファイル名: cp031634.compsig; cp031634.exe; cp031634.md5

拡張

最初のリリース

オンラインROMフラッシュコンポーネント for Windows (x64) - HPE Apollo 4200 Gen9バックプレーンエキスパンダーファームウェア

バージョン: 1.50 **(オプション)**
ファイル名: cp035218.exe; cp035218.md5

重要な注意！

- ファームウェアがバージョン1.03またはそれ以前からアップグレードされた場合には、電源再投入/コールドリブートが必要です。

オンラインROMフラッシュコンポーネント for Windows (x64) - HPE Apollo 45xx Gen10バックプレーンエキスパンダーファームウェア

バージョン: 1.56 **(オプション)**
ファイル名: cp034415.compsig; cp034415.exe; cp034415.md5

拡張

- ドライブゾーニングをサポートします

オンラインROMフラッシュコンポーネント for Windows (x64) - HPE Apollo 45xx Gen9バックプレーンエキスパンダーファームウェア

バージョン: 2.08 (B) **(オプション)**
ファイル名: cp034911.exe; cp034911.md5

重要な注意！

- すでにファームウェアバージョン2.08をインストールしている場合、2.08(B)にアップデートする必要はありません。
- バージョン1.03以前からのファームウェアアップグレードを有効にするために、サーバーの電源コードを1度抜いて、再度挿してください。

拡張

HPEデジタル署名を追加しました

オンラインROMフラッシュコンポーネント for Windows (x64) - HPE Express Bay Enablement Switch Card

バージョン: 1.78 (B) **(オプション)**
ファイル名: cp034796.exe; cp034796.md5

重要な注意！

- すでにファームウェアバージョン1.78をインストールしている場合、1.78(B)にアップデートする必要はありません。
- アップデートを有効にするには、インストール後に電源再投入/コールドリブートが必要です。

事前要件

- このフラッシュコンポーネントを使用する前に、"HP ProLiant iLO 3/4 Channel Interfaceドライバー"がインストールされて実行されている必要があります。 ドライバーが実行されていない場合、次のエラーメッセージが表示されます。

  "Setup is unable to load a setup DLL"

- HP ProLiant iLOファームウェアバージョンは、v2.20以降である必要があります。 HP ProLiant iLOファームウェアがv2.20より古い場合、以下のエラーメッセージを受け取ります。

  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.

拡張

HPEデジタル署名を追加しました

オンラインROMフラッシュコンポーネント for Windows (x64) - Smartアレイ H240ar、H240、

H240nr、H241、H244br、P240nr、P244br、P246br、P440ar、P440、P441、P542D、P741m、P840、P840arおよびP841

バージョン: 6.60 **(推奨)**
ファイル名: cp035731.exe; cp035731.md5

修正

- QueryAsynchronousEventが不適切な応答データを提供する可能性がある問題
- 数回の再起動後にキャッシュが無効になる可能性があるという問題

拡張

- 大きな容量サイズのスマートキャッシュに対するサポートが追加されました

オンラインROMフラッシュコンポーネント for Windows (x64) - SmartアレイP220i、P222、P420i、P420、P421、P721m、およびP822

バージョン: 8.32 (B) **(推奨)**
ファイル名: cp034910.exe; cp034910.md5

重要な注意!

- すでにファームウェアバージョン8.32をインストールしている場合、8.32(B)にアップデートする必要はありません。

拡張

HPEデジタル署名を追加しました

オンラインROMフラッシュコンポーネント for Windows (x64) - SmartアレイP230i、P430、P431、P731m、P830i および P830

バージョン: 4.54 **(オプション)**
ファイル名: cp034040.exe; cp034040.md5

修正

- DDRキャッシュは数回起動した後に、ランダムに無効になります。
- 元のドライブが障害予測を持つと特定された場合、hot-inserted交換ドライブは、障害予測として表示される可能性があります。
- コントローラーキャッシュモジュールは、Smartストレージバッテリーが取り外されているかシステムがオンラインの時に障害が発生すると、バックアップ電源なしでの書き込みキャッシングの有効化に以前はSSAが使用されていたとしても、永久的に無効としてマークが付けられる可能性があります。
- 先読みと読み取り入力が順番に実行されるときにスマートキャッシュがフラッシュ操作を保留中であるため、コントローラーが応答しなくなることがあります。
- RAID6ボリュームのサーフェース・スキャン中にパリティエラーが見つかった場合、システムが応答を停止することがあります。(POST Lockup 0x13)
- 接続されたドライブがスピンダウンされた場合は、システムファンが100%に到達する可能性があります
- コントローラーの障害が発生した後で、コントローラークラッシュダンプが収集されない可能性がある問題

オンラインROMフラッシュコンポーネント for Windows x64 - HPEホストバスアダプターH221

バージョン: 15.10.10.00 (C) **(オプション)**
ファイル名: cp034832.exe; cp034832.md5

重要な注意！

このドライバーコンポーネントは、H221コントローラー搭載のGen9サーバーのみをサポートし、コントローラーはGen9サーバーでのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしません。

サポートしているデバイスおよび機能

このドライバーコンポーネントは、H221コントローラー搭載のGen9サーバーのみをサポートし、コントローラーはGen9サーバーでのD2600、D2700、およびD6000ディスクエンクロージャーへの接続をサポートしません。

オンラインROMフラッシュコンポーネントfor Linux (x64) – HPE D2500sbストレージブレード用HPE SASエキスパンダーファームウェア

バージョン: 2.00 (A) **(オプション)**
ファイル名: 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

拡張

最初のリリース

オンラインROMフラッシュコンポーネントfor VMware ESXi - HPE Apollo 2000 Gen10バックプレーンエキスパンダーファームウェア

バージョン: 1.00 (B) **(オプション)**
ファイル名: CP036724.compsig; CP036724.zip

重要な注意!

ファームウェアバージョン1.00を既にインストールしている場合、1.00 (B)へアップデートする必要はありません。

拡張

- Smart Update Managerとの統合を強化しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - HPE Apollo 45xx Gen10バックプレーンエキスパンダーファームウェア

バージョン: 1.56 (B) **(オプション)**
ファイル名: CP036717.compsig; CP036717.zip

重要な注意!

ファームウェアバージョン1.56をすでにインストールしている場合、1.56 (B)へアップデートする必要はありません。

拡張

- Smart Update Managerとの統合を強化しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - HPE Apollo 45xx Gen9バックプレーンエキスパンダーファームウェア

バージョン: 2.08 **(オプション)**
ファイル名: CP031316.zip

重要な注意！

- バージョン1.03以前からのファームウェアアップグレードを有効にするために、サーバーの電源コードを1度抜いて、再度挿してください。

拡張

- デバッグ機能を強化しました。
- VMware vSphere 2016 OSのサポートを追加しました。
- Smart Update Managerとの統合を強化しました。

オンラインROMフラッシュコンポーネントfor VMware ESXi - HPE D2500sbストレージブレード用HPE SASエキスパンダーファームウェア

バージョン: 2.00 (B) **(オプション)**
ファイル名: CP036701.compsig; CP036701.zip

重要な注意！

ファームウェアバージョン2.00をすでにインストールしている場合、2.00 (B)へアップデートする必要はありません。

- ESXi6.0を使用するには、アップグレード3以降である必要があります。以前のバージョンのOSには必要なSmartPQIドライバーがありません。

事前要件

ESXi6.0を使用するには、アップグレード3以降である必要があります。以前のバージョンのOSには必要なSmartPQIドライバーがありません。

拡張

- Smart Update Managerとの統合を強化しました。

オンラインROMフラッシュコンポーネントfor Windows (x64) - HPE Apollo 2000 System - SASエキスパンダー

バージョン: 1.00 (D) **(推奨)**
ファイル名: cp034756.exe; cp034756.md5

重要な注意!

- すでに以前のファームウェアバージョン1.00をインストールしている場合、1.00(D)にアップデートする必要はありません。

拡張

HPEデジタル署名を追加しました

オンラインROMフラッシュコンポーネントfor Windows (x64) - HPE D2500sbストレージブレード用HPE SASエキスパンダーファームウェア

バージョン: 2.00 **(オプション)**
ファイル名: cp036364.compsig; cp036364.exe; cp036364.md5

拡張

最初のリリース

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - HPE Apollo 45xx Gen9バックプレーンエキスパンダーファームウェア

バージョン: 2.08 **(オプション)**
ファイル名: rpm/RPMS/x86_64/firmware-smartarray-7bdfcd246b-2.08-1.1.x86_64.rpm

重要な注意！

- バージョン1.03以前からのファームウェアアップグレードを有効にするために、サーバーの電源コードを1度抜いて、再度挿してください。

拡張

- デバッグ機能を強化しました。
- Smart Update Managerとの統合を強化しました。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - Smartアレイ H240ar、H240、H240nr、H241、H244br、P240nr、P244br、P246br、P440ar、P440、P441、P542D、P741m、P840、P840arおよびP841

バージョン: 6.60 (B) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-smartarray-ea3138d8e8-6.60-2.1.x86_64.rpm

重要な注意！

- 正しく検出されるために、いくつかのコントローラーは、コントローラーファームウェアをアップグレードする前にSmartアレイドライバーの新しいバージョンのインストールが必要な場合があります。 インストールされていない場合、コンポーネントはリターンコード3で失敗します。
- Red Hat Enterprise Linux 7.1オペレーティングシステムを実行するシステムを起動すると、HP Smartアレイコントローラーが認識されないことがあります。この問題は、sgドライバーをシステムブート時にロードしないOSでの変更に起因します。この問題を回避するには、sgドライバーをロードする"**modprobe sg**"コマンドを手動で発行します。sgドライバーがロードされた後、/dev/sg* デバイスが存在するようになり、sgドライバーがSCSIデバイスにアクセスするために使用可能になります。

サプリメンタルアップデート / オンラインROMフラッシュコンポーネント for Linux (x64) - Smartアレイ P220i、P222、P420i、P420、P421、P721m、およびP822

バージョン: 8.32 **(推奨)**
ファイル名: rpm/RPMS/x86_64/hp-firmware-smartarray-46a4d957a7-8.32-1.1.x86_64.rpm

重要な注意！

- Red Hat Enterprise Linux 7.1オペレーティングシステムを実行するシステムを起動すると、HP Smartアレイコントローラーが認識されないことがあります。 この問題は、sgドライバーをシステムブート時にロードしないOSでの変更に起因します。 この問題を回避するには、sgドライバーをロードする"**modprobe sg**"コマンドを手動で発行します。 sgドライバーがロードされた後、/dev/sg* デバイスが存在する必要があり、sgドライバーがSCSIデバイスにアクセスするために使用することができます。

修正

システムは、ベースコードファームウェアによって返される完了について、RAIDスタックスレッドがキューをポーリングしているライブロック状況のために、ロックアップコードを表示せずに応答を停止することがあります。

拡張

ドライブ温度レポート機能の精度が改善されました。

サプリメンタルアップデート/Linux(x64)用オンラインROMフラッシュコンポーネント - HPE Smartアレイ P408i-p、P408e-p、P408i-a、P408i-c、E208i-p、E208e-p、E208i-c、E208i-a、P204i-c、P204i-b、P816i-a、およびP416ie-m SR Gen10

バージョン: 1.65 **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-smartarray-f7c07bdbbd-1.65-1.1.x86_64.compsig; rpm/RPMS/x86_64/firmware-smartarray-f7c07bdbbd-1.65-1.1.x86_64.rpm

修正

- システムがPOST中に応答しなくなり、OSのロードに失敗することがありました。この問題は、システム BIOSのバージョンが1.40以降の場合に発生する可能性が高くなります。ただし、以前のBIOSバージョンを実行しているシステムでもこの問題が発生する可能性があります。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - HPE 12 Gb/s SASエキスパンダーファームウェア for HPE Smartアレイコントローラーおよび HPE HBAコントローラー

バージョン: 4.02 **(オプション)**
ファイル名: 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

重要な注意！

- ファームウェアがバージョン1.31またはそれ以前からアップグレードされた場合には、電源再投入/コールドリブートが必要です。

修正

- エンクロージャーのターゲットおよびLUNアドレスを適切な固有の値に変更しました。以前では、これらのアドレスはベイ#1のSATAドライブと競合し、このことがStorage Spaces Directなどのソフトウェア定義ストレージソリューションに影響していました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - HPE Apollo 45xx Gen10バックプレーンエキスパンダーファームウェア

バージョン: 1.56 **(オプション)**
ファイル名: 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

拡張

- ドライブゾーニングをサポートします

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - HPE Express Bay Enablement Switch Card

バージョン: 1.78 **(オプション)**
ファイル名: firmware-smartarray-94189dca85-1.78-1.1.x86_64.rpm

重要な注意！

- アップデートを有効にするには、インストール後に電源再投入/コールドリブートが必要です。

事前要件

- HPE Express Bay Enablement Switch CardファームウェアSmartコンポーネントの前回リリースでは、iLO 3/4チャネルインターフェイスドライバーへの依存が記録されました。このドライバーは、以下のLinux OSに含まれるようにな

りました。

Red Hat Enterprise Linux 7 Server

Red Hat Enterprise Linux 6 Server (x86-64)

SUSE Linux Enterprise Server 12

- HP ProLiant iLOファームウェアバージョン2.20以降が必要。HP ProLiant iLOファームウェアがv2.20以前の場合、次のエラーメッセージを受信します。

  依存性の確認に失敗しました。

  現在のバージョン*:iLOx x.xx*

  必要な最小バージョン*:iLO4 2.20*

  必要なハードウェアがシステムに存在しないかソフトウェア/ファームウェアがこのシステムに適用しないため、ソフトウェアはこのシステムにインストールされません。

修正

- Seagate NVMeハードドライブの温度ステータスを修正しました。

サプリメンタルアップデート/オンラインROMフラッシュコンポーネント for Linux (x64) - Smartアレイ P230i、P430、P431、P731m、P830i および P830

バージョン: 4.54 (B) **(推奨)**
ファイル名: rpm/RPMS/x86_64/firmware-smartarray-112204add8-4.54-2.1.x86_64.rpm

重要な注意！

- Red Hat Enterprise Linux 7.1オペレーティングシステムを実行するシステムを起動すると、HP Smartアレイコントローラーが認識されないことがあります。 この問題は、sgドライバーをシステムブート時にロードしないOSでの変更に起因します。 この問題を回避するには、sgドライバーをロードする"**modprobe sg**"コマンドを手動で発行します。 sgドライバーがロードされた後、/dev/sg* デバイスが存在する必要があり、sgドライバーがSCSIデバイスにアクセスするために使用することができます。

修正

- DDRキャッシュは数回起動した後に、ランダムに無効になります。
- 元のドライブが障害予測を持つと特定された場合、hot-inserted交換ドライブは、障害予測として表示される可能性があります。
- コントローラーキャッシュモジュールは、Smartストレージバッテリーが取り外されているかシステムがオンラインの時に障害が発生すると、バックアップ電源なしでの書き込みキャッシングの有効化に以前はSSAが使用されていたとしても、永久的に無効としてマークが付けられる可能性があります。
- 先読みと読み取り入力が順番に実行されるときにスマートキャッシュがフラッシュ操作を保留中であるため、コントローラーが応答しなくなることがあります。
- RAID6ボリュームのサーフェース・スキャン中にパリティエラーが見つかった場合、システムが応答を停止することがあります。(POST Lockup 0x13)
- 接続されたドライブがスピンダウンされた場合は、システムファンが100%に到達する可能性があります
- コントローラーの障害が発生した後で、コントローラークラッシュダンプが収集されない可能性がある問題

ファームウェア - ストレージファイバーチャネル

先頭

Emulexファイバーチャネルホストバスアダプター for VMware vSphere 6.5用HPEファームウェアフラッシュ

バージョン: 2018.09.02 **(推奨)**

ファイル名: CP037460.compsig; CP037460.zip

重要な注意！

リリースノート:

HPE StoreFabric Emulex アダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

ファイバーチャネルとコンバージドネットワークアダプターをアップデートするためのコンポーネントがあります。これは、ファイバーチャネルのアップデートコンポーネントです。

下記のサポートを追加しました:

16/32 Gb HBA/メザニンユニバーサルブートをアップデートしました
16 Gb HBA/メザニンユニバーサルブートをアップデートしました。
8Gb HBA/メザニンユニバーサルブートをアップデートしました。

含まれるもの:

16/32 Gb HBA/メザニンユニバーサルブート11.4.334.10
16 Gb HBA/メザニンユニバーサルブート11.4.334.11

8 Gbスタンドアップ/メザニンファームウェア2.10X6

8 Gbスタンドアップ/メザニンユニバーサルブートイメージ11.40a13(11.4.305.0 BIOS、11.4.344.0 UEFI)

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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 Linux (x64)

バージョン: 2018.09.02 **(推奨)**
ファイル名: RPMS/x86_64/firmware-fc-emulex-2018.09.02-1.3.x86_64.compsig; RPMS/x86_64/firmware-fc-emulex-2018.09.02-1.3.x86_64.rpm

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

ファームウェアアップデートは、インボックスまたはOut of Box(OOB)ドライバーを使用して実行できます。 サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

このファームウェアコンポーネントが展開のためにSUMで識別される前に、HPEで提供しているイネーブルメントキットをインストールする必要があります。

OOBドライバーおよびイネーブルメントキットは、http://www.hpe.com/servers/spp/downloadのService Pack for ProLiant(SPP)から入手できます。

イネーブルメントキットは、OSインストールメディアからlibHBAAPIパッケージをインストールしたターゲット環境を必要とします。

FCドライバーキットをインストールし、再起動してからイネーブルメントキットをインストールしてください。

追加の要件:

フラッシュエンジンを動作させるためにsyslogデーモンが実行されている環境が必要です
コンポーネントでEmulexホストバスアダプター(HBA)を検出できるようにするには、32-bit netlink library(libnl.so)がインストールされている環境が必要です

拡張

ファイバーチャネルおよびコンバージドネットワークアダプターをアップデートする別々のコンポーネントがあります。 これは、ファイバーチャネルアップデートコンポーネントです。

16 Gb HBA/メザニンユニバーサルブートをアップデートしました。
32 Gb HBAユニバーサルブートをアップデートしました。
8Gb HBA/メザニンブートBIOSをアップデートしました。

含まれるもの:

16 Gb HBA/メザニンユニバーサルブート 11.4.199.0
16/32 GB HBAユニバーサルブート11.4.199.0

8 Gb Gen8メザニン (LPe1205A) ファームウェア2.03X14
8 Gb スタンドアップファームウェア 2.03x14
8 Gb メザニンファームウェア 2.03x14
8 Gb HBA/メザニンブートイメージ11.40A5(11.4.170.0 BIOS、11.4.185.0 UEFI)

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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 6.0

バージョン: 2018.09.02 **(推奨)**
ファイル名: CP037461.compsig; CP037461.zip

重要な注意！

リリースノート:

HPE StoreFabric Emulex アダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

ファイバーチャネルとコンバージドネットワークアダプターをアップデートするためのコンポーネントがあります。これは、ファイバーチャネルのアップデートコンポーネントです。

下記のサポートを追加しました:

16/32 Gb HBA/メザニンユニバーサルブートをアップデートしました
16 Gb HBA/メザニンユニバーサルブートをアップデートしました。
8Gb HBA/メザニンユニバーサルブートをアップデートしました。

含まれるもの:

16/32 Gb HBA/メザニンユニバーサルブート11.4.334.10
16 Gb HBA/メザニンユニバーサルブート11.4.334.11

8 Gbスタンドアップ/メザニンファームウェア2.10x6

8 Gbスタンドアップ/メザニンユニバーサルブートイメージ11.40a13(11.4.305.0 BIOS、11.4.344.0 UEFI)

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター

- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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

バージョン: 2018.09.02 **(推奨)**
ファイル名: cp037458.compsig; cp037458.exe

重要な注意！

リリースノート:
HPE StoreFabric Emulexアダプターリリースノート

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

このファームウェアコンポーネントが展開のためにSUMで識別される前に、HPEで提供しているEmulexドライバーをインストールする必要があります。OOBドライバーは、 http://www.hpe.com/servers/spp/download/ のService Pack for ProLiant(SPP)から入手できます。

拡張

ファイバーチャネルおよびコンバージドネットワークアダプターをアップデートする別々のコンポーネントがあります。 これは、ファイバーチャネルアップデートコンポーネントです。

16 Gb HBA/メザニンユニバーサルブートをアップデートしました。
32 Gb HBAユニバーサルブートをアップデートしました。
8Gb HBA/メザニンブートBIOSをアップデートしました。

含まれるもの:

16 Gb HBA/メザニンユニバーサルブート 11.4.199.0

16/32 GB HBAユニバーサルブート11.4.199.0

8 Gb Gen8メザニン (LPe1205A) ファームウェア2.03X14
8 Gb スタンドアップファームウェア 2.03x14
8 Gb メザニンファームウェア 2.03x14
8 Gb HBA/メザニンブートイメージ11.40A5(11.4.170.0 BIOS、11.4.185.0 UEFI)

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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 Online Flash for QLogic Fibre Channel Host Bus Adapters - Windows 2012/2012R2/2016 (x86_64)

バージョン: 2018.06.01 **(推奨)**
ファイル名: cp034231.compsig; cp034231.exe

重要な注意！

リリースノート:
HPE StoreFabric QLogic アダプターリリースノート

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

OOBドライバーは、http://www.hpe.com/servers/spp/downloadのService Pack for ProLiant(SPP)から入手できます。

修正

8Gbスタンドアップ &8Gbメザニン

BIOS

- メンテナンスアップデート:

UEFI

- Linux起動中にDMAエラーの原因となったOCBBバグを修正しました。
- 3PARストレージアレイでのWin2012起動問題を修正しました。

16Gbスタンドアップ &16Gbメザニン

BIOS

- FA_BLUNを有効化しているときに、直接接続されたLUNを構成するできるようにするコードを追加しました。
- PCIアドレスが正しくセットアップされていない場合のcheck_mem64ルーチンの予測不能な動作を修正しました。
- FlexAddressが失敗する原因となるバグを修正しました。

UEFI

- QMH2672アダプターのHII Load Defaults問題を修正しました。 HII Loadでは、既定で[Adapter Settings]メニューに項目を追加しなくなりました
- Linuxブート中にDMAエラーを発生したOCBBバグを修正しました。
- ターゲットアレイでのWin2012起動問題を修正しました。

拡張

16Gbスタンドアップ &16Gbメザニン

BIOS

- POST Discovery Mode機能を追加しました

UEFI

- POST Discovery Mode機能を追加しました
- Scan Fibre Devices HIIフィールドを追加しました

32Gbスタンドアップ &16Gbメザニン

BIOS

- POST Discovery Mode機能を追加しました

UEFI

- POST Discovery Mode機能を追加しました

8 Gb、16 Gbおよび32 Gb製品のためのファームウェア/BIOS/UEFIパッケージをアップデートしました。

- 8 Gb HBA/メザニン
  - パッケージ3.76.08
  - ファームウェア8.05.00
  - UEFI 6.55
  - BIOS 3.56
- 16 Gb HBA/メザニン
  - パッケージ6.01.45
  - ファームウェア8.05.64
  - UEFI 6.55
  - BIOS 3.43
- 16/32 Gb
  - パッケージ01.70.59

- ファームウェア8.05.64
- UEFI 6.39
- BIOS 3.54

サポートしているデバイスおよび機能

このファームウェアは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

QLogicファイバーチャネルホストバスアダプター for VMware vSphere 6.0用HPEファームウェアフラッシュ

バージョン: 2018.09.01 **(推奨)**
ファイル名: CP035931.compsig; CP035931.zip

重要な注意！

HPE StoreFabric QLogic アダプターリリースノート

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

展開のためにHPE SUMによりこのファームウェアコンポーネントが識別される前に、SUMが供給するQLogicドライバーをインストールする必要があります。OOBドライバーは、 http://www.hpe.com/servers/spp/download/ のService Pack for ProLiant(SPP)から入手できます。

修正

Fixed the following

拡張

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 01.70.79
        - Firmware 8.07.16
        - UEFI 6.47
        - BIOS 3.54

サポートしているデバイスおよび機能

このファームウェアは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

QLogicファイバーチャネルホストバスアダプター for VMware vSphere 6.5用HPEファームウェアフラッシュ

バージョン: 2018.09.01 **(推奨)**
ファイル名: CP035932.compsig; CP035932.zip

重要な注意！

HPE StoreFabric QLogic アダプターリリースノート

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

展開のためにHPE SUMによりこのファームウェアコンポーネントが識別される前に、SUMが供給するQLogicドライバーをインストールする必要があります。OOBドライバーは、 http://www.hpe.com/servers/spp/download/ のService Pack for ProLiant(SPP)から入手できます。

修正

8Gbスタンドアップ &8Gbメザニン

BIOS

- メンテナンスアップデート:

UEFI

- Linux起動中にDMAエラーの原因となったOCBBバグを修正しました。
- 3PARストレージアレイでの Win2012起動問題を修正しました。

16Gbスタンドアップ &16Gbメザニン

BIOS

- FA_BLUNを有効化しているときに、直接接続されたLUNを構成するできるようにするコードを追加しました。
- PCIアドレスが正しくセットアップされていない場合のcheck_mem64ルーチンの予測不能な動作を修正しました。
- FlexAddressが失敗する原因となるバグを修正しました。

UEFI

- QMH2672アダプターのHII Load Defaults問題を修正しました。 HII Loadでは、既定で[Adapter Settings]メニューに項目を追加しなくなりました
- Linuxブート中にDMAエラーを発生したOCBBバグを修正しました。
- ターゲットアレイでのWin2012起動問題を修正しました。

拡張

16Gbスタンドアップ &16Gbメザニン

BIOS

- POST Discovery Mode機能を追加しました

UEFI

- POST Discovery Mode機能を追加しました
- Scan Fibre Devices HIIフィールドを追加しました

32Gbスタンドアップ &16Gbメザニン

BIOS

- POST Discovery Mode機能を追加しました

UEFI

- POST Discovery Mode機能を追加しました

8 Gb、16 Gbおよび32 Gb製品のためのファームウェア/BIOS/UEFIパッケージをアップデートしました。

- 8 Gb HBA/メザニン
  - パッケージ3.76.08
  - ファームウェア8.05.00
  - UEFI 6.55
  - BIOS 3.56
- 16 Gb HBA/メザニン

        - パッケージ6.01.45
        - ファームウェア8.05.64
        - UEFI 6.55
        - BIOS 3.43

    - 16/32 Gb
        - パッケージ01.70.59
        - ファームウェア8.05.64
        - UEFI 6.39
        - BIOS 3.54

サポートしているデバイスおよび機能

このファームウェアは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

QLogicファイバーチャネルホストバスアダプター用HPEファームウェアフラッシュ - Linux (x86_64)

バージョン: 2018.09.01 **(推奨)**
ファイル名: RPMS/x86_64/firmware-fc-qlogic-2018.09.01-1.1.x86_64.compsig; RPMS/x86_64/firmware-fc-qlogic-2018.09.01-1.1.x86_64.rpm

重要な注意！

リリースノート:
HPE StoreFabric QLogic アダプターリリースノート

事前要件

ファームウェアアップデートは、インボックスまたはOut of Box(OOB)ドライバーを使用して実行できます。 サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

このファームウェアコンポーネントが展開のためにSUMで識別される前に、HPEで提供しているイネーブルメントキットをインストールする必要があります。

OOBドライバーおよびイネーブルメントキットは、http://www.hpe.com/servers/spp/downloadのService Pack for ProLiant(SPP)から入手できます。

修正

8Gbスタンドアップ &8Gbメザニン

拡張

8 Gb、16 Gbおよび32 Gb製品のためのファームウェア/BIOS/UEFIパッケージをアップデートしました。

- 8 Gb HBA/メザニン
  - パッケージ3.76.08
  - ファームウェア8.05.00
  - UEFI 6.55
  - BIOS 3.56

- 16 Gb HBA/メザニン
  - パッケージ6.01.45
  - ファームウェア8.05.64
  - UEFI 6.55
  - BIOS 3.43

- 16/32 Gb
  - パッケージ01.70.59
  - ファームウェア8.05.64
  - UEFI 6.39
  - BIOS 3.54

サポートしているデバイスおよび機能

このファームウェアは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

ファームウェア - システム

先頭

Linux用オンラインフラッシュコンポーネント - Gen10 NVMeバックプレーンPICファームウェア

バージョン: 1.20 (D) **(オプション)**

ファイル名: 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

事前要件

iLO 5バージョン1.10以降が必要です。

修正

ファームウェアパッケージバージョン1.20(D) では、次の問題に対処しました。

- OneViewの使用時に、ファームウェアをバージョン1.18から1.20にアップグレードする試みに失敗しました。

注:ターゲットデバイスがすでにファームウェアバージョン1.20にアップデートされている場合は、ファームウェアアップデート1.20(D) を適用する必要はありません。

拡張

バージョン1.20(C) には、次のサポートが追加されました。バージョン1.20(D) には、追加された新機能はありません。

- HPE ProLiant XL270d Gen10サーバーのサポートを追加しました。

Linux用オンラインフラッシュコンポーネント - NVMeバックプレーンPICファームウェア

バージョン: 8.4 (C) **(オプション)**
ファイル名: RPMS/i386/firmware-nvmebackplane-8.4-3.1.i386.rpm

事前要件

iLO 4バージョン2.50以降が必要です。

拡張

- Service Pack for ProLiantバージョン2017.07.0をサポートするためにアップデートされました

  注記:システムが以前にバージョン8.4にアップデートされている場合、8.4 (C)にアップデートする必要はありません。

VMware 用オンラインフラッシュコンポーネント - NVMeバックプレーンPICファームウェア

バージョン: 8.4 (C) **(オプション)**
ファイル名: CP033323.compsig; CP033323.zip

事前要件

iLO 4バージョン2.50以降が必要です。

拡張

- Service Pack for ProLiantバージョン2017.07.0をサポートするためにアップデートされました

  注記:システムが以前にバージョン8.4にアップデートされている場合、8.4 (C)にアップデートする必要はありません。

オンラインフラッシュコンポーネント for Windows x64 - NVMeバックプレーンPICファームウェア

バージョン: 8.4 (D) **(オプション)**
ファイル名: cp034942.exe

事前要件

iLO 4バージョン2.50以降が必要です。

オンラインフラッシュコンポーネントfor Windows x64 - Gen10 NVMeバックプレーンPICファームウェア

バージョン: 1.20 (C) **(オプション)**
ファイル名: cp036570.compsig; cp036570.exe

事前要件

iLO 5バージョン1.10以降が必要です。

修正

ファームウェアパッケージバージョン1.20(C) では、次の問題に対処しました。

- OneViewの使用時に、ファームウェアをバージョン1.18から1.20にアップグレードする試みに失敗しました。

注:ターゲットデバイスがすでにファームウェアバージョン1.20にアップデートされている場合は、ファームウェアアップデート1.20(C) を適用する必要はありません。

拡張

バージョン1.20(B) には、次のサポートが追加されました。バージョン1.20(C) には、追加された新機能はありません。

- HPE ProLiant XL270d Gen10サーバーのサポートを追加しました。

ファームウェア(認証が必要) - ストレージコントローラー

先頭

HP D6000 6Gb SASディスクエンクロージャーROMフラッシュコンポーネント for Windows (x64)

バージョン: 2.98 **(クリティカル)**
ファイル名: cp029908.exe; cp029908.md5

重要な注意！

重要: ファームウェアのアップグレードは、システムの全てのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

重要: 電源入/切シーケンスには、構成の完全性を維持することが重要です。詳細は、"HP D6000 ディスクエンクロージャーユーザーガイド"の文書を参照してください。

警告！ このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注意:すべてのファームウェアフラッシュ進行メッセージは、%systemdrive%¥CPQSYSTEM¥Log¥Verbose.logに記録され、フラッシュの概要は、%systemdrive%¥CPQSYSTEM¥Log¥cpqsetup.logに記録されます。

事前要件

重要: ファームウェアのアップグレードは、システムの全てのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！ このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注意:すべてのファームウェアフラッシュ進行メッセージは、%systemdrive%¥CPQSYSTEM¥Log¥Verbose.logに記録され、フラッシュの概要は、%systemdrive%¥CPQSYSTEM¥Log¥cpqsetup.logに記録されます。

修正

以下の問題がこのファームウェアのバージョンで修正されます:

12GB SAS HDDがエンクロージャー内に搭載されている場合、ディスクディスカバリをサポートするために、SAS エキスパンダーの設定を変更しました。

サポートしているデバイスおよび機能

HP D6000 ディスクエンクロージャーは、以下のデバイスの後部で接続できます:

- HP H222ホストバスアダプター
- HP H221ホストバスアダプター
- HP H241 Smart ホストバスアダプター
- HP SmartアレイP731mコントローラー
- HP SmartアレイP741mコントローラー
- HP SmartアレイP721mコントローラー
- HP SmartアレイP441コントローラー
- HP SmartアレイP431コントローラー
- HP SmartアレイP822コントローラー
- HP SmartアレイP841コントローラー
- HP SmartアレイP421コントローラー

HP D2600/D2700 6Gb SASディスクエンクロージャーROMフラッシュコンポーネント for Linux (x64)

バージョン: 0150 (B) **(推奨)**
ファイル名: RPMS/x86_64/hp-firmware-d2600-d2700-0150-2.1.x86_64.rpm

重要な注意！

現在デバイスが150ファームウェアを実行している場合、150(B)へファームウェアをアップグレードする必要はありません

重要:ファームウェアのアップグレードは、システムの全てのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注: ディスクエンクロージャーがカスケードされたとき、1つのエンクロージャーのI/OモジュールAは、その後のエンクロージャーのI/OモジュールAに接続されます。ファームウェアのアップデート中、カスケードされたディスクエンクロージャー内のI/OモジュールAは、自動的にアップデートされます。

デュアルドメイン構成で、ターゲットディスクエンクロージャーとカスケードディスクエンクロージャーのI/Oモジュールは、ファームウェアインストール処理の間、自動的にアップデートされます。

すべてのファームウェアフラッシュの進捗メッセージは、/var/cpq/Component.logに記録されます。

事前要件

重要: ファームウェアのアップグレードは、システムの全てのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！ このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注: ディスクエンクロージャーがカスケードされたとき、1つのエンクロージャーのI/OモジュールAは、その後のエンクロージャーのI/OモジュールAに接続されます。ファームウェアのアップデート中、カスケードされたディスクエンクロージャー内のI/OモジュールAは、自動的にアップデートされます。

デュアルドメイン構成で、ターゲットディスクエンクロージャーとカスケードディスクエンクロージャーのI/Oモジュールは、ファームウェアインストール処理の間、自動的にアップデートされます。

すべてのファームウェアフラッシュの進捗メッセージは、/var/cpq/Component.logに記録されます。

修正

このバージョンでは、次の修正が追加されています。

誤ったアルゴリズムによるFAULT_SENSEDビットに関するアクションを削除しました。

サポートしているデバイスおよび機能

D2600 / D2700エンクロージャーは、どのHPストレージコントローラーとホストバスアダプターにも接続できます。

- HP H222 ホストバスアダプター
- HP H221 ホストバスアダプター
- HP H241 Smartホストバスアダプター
- HP SmartアレイP812コントローラー
- HP SmartアレイP822コントローラー
- HP SmartアレイP841コントローラー
- HP SmartアレイP441コントローラー
- HP SmartアレイP431コントローラー
- HP SmartアレイP421コントローラー
- HP SmartアレイP411コントローラー
- HP SmartアレイP212コントローラー
- HP SmartアレイP222コントローラー

HP D2600/D2700 6Gb SASディスクエンクロージャーROMフラッシュコンポーネント for Windows (x64)

バージョン: 0150 (B) **(推奨)**
ファイル名: cp028806.exe

重要な注意！

現在デバイスが150ファームウェアを実行している場合、150(B)へファームウェアをアップグレードする必要はありません

重要: ファームウェアのアップグレードは、システムの全てのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注: ディスクエンクロージャーがカスケードされたとき、1つのエンクロージャーのI/OモジュールAは、その後のエンクロージャーのI/OモジュールAに接続されます。ファームウェアのアップデート中、カスケードされたディスクエンクロージャー内のI/OモジュールAは、自動的にアップデートされます。

デュアルドメイン構成で、ターゲットディスクエンクロージャーとカスケードディスクエンクロージャーのI/Oモジュールは、ファームウェアインストール処理の間、自動的にアップデートされます。

すべてのファームウェアフラッシュ進行メッセージは、%systemdrive%¥CPQSYSTEM¥Log¥D2000.logに記録され、フラッシュの要約は、%systemdrive%¥CPQSYSTEM¥Log¥cpqsetup.logに記録されます。

事前要件

重要: ファームウェアのアップグレードは、システムの全てのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！ このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注: ディスクエンクロージャーがカスケードされたとき、1つのエンクロージャーのI/OモジュールAは、その後のエンクロージャーのI/OモジュールAに接続されます。ファームウェアのアップデート中、カスケードされたディスクエンクロージャー内のI/OモジュールAは、自動的にアップデートされます。

デュアルドメイン構成で、ターゲットディスクエンクロージャーとカスケードディスクエンクロージャーのI/Oモジュールは、ファームウェアインストール処理の間、自動的にアップデートされます。

すべてのファームウェアフラッシュ進行メッセージは、%systemdrive%¥CPQSYSTEM¥Log¥D2000.logに記録され、フラッシュの要約は、%systemdrive%¥CPQSYSTEM¥Log¥cpqsetup.logに記録されます。

修正

このバージョンでは、次の修正が追加されています。

誤ったアルゴリズムによるFAULT_SENSEDビットに関するアクションを削除しました。

サポートしているデバイスおよび機能

D2600 / D2700エンクロージャーは、どのHPストレージコントローラーとホストバスアダプターにも接続できます。

- HP H222 ホストバスアダプター
- HP H221 ホストバスアダプター
- HP H241 Smartホストバスアダプター
- HP SmartアレイP812コントローラー
- HP SmartアレイP822コントローラー
- HP SmartアレイP841コントローラー
- HP SmartアレイP441コントローラー
- HP SmartアレイP431コントローラー
- HP SmartアレイP421コントローラー
- HP SmartアレイP411コントローラー
- HP SmartアレイP212コントローラー
- HP SmartアレイP222コントローラー

HP D6000 6Gb SASディスクエンクロージャーROMフラッシュコンポーネント for Linux (x64)

バージョン: 2.98 **(クリティカル)**
ファイル名: RPMS/x86_64/hp-firmware-smartarray-d6000-2.98-1.1.x86_64.rpm

重要な注意！

重要: ファームウェアのアップグレードは、システムの全てのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

重要: 電源入/切シーケンスには、構成の完全性を維持することが重要です。詳細は、"HP D6000 ディスクエンクロージャーユーザーガイド"の文書を参照してください。

警告！このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注意:すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/Verbose.log に記録され、フラッシュの概要は、/var/cpq/Component.logに記録されます。

事前要件

重要: ファームウェアのアップグレードは、システムの全てのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！ このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注意:すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/Verbose.logに記録され、フラッシュの概要は、/var/cpq/Component.logに記録されます。

修正

以下の問題がこのファームウェアのバージョンで修正されます:

12GB SAS HDDがエンクロージャー内に搭載されている場合、ディスクディスカバリをサポートするために、SAS エキスパンダーの設定を変更しました。

サポートしているデバイスおよび機能

HP D6000 ディスクエンクロージャーは、以下のデバイスの後部で接続できます:

- HP H222ホストバスアダプター
- HP H221ホストバスアダプター
- HP H241 Smart ホストバスアダプター
- HP SmartアレイP731mコントローラー
- HP SmartアレイP741mコントローラー
- HP SmartアレイP721mコントローラー
- HP SmartアレイP441コントローラー
- HP SmartアレイP431コントローラー
- HP SmartアレイP822コントローラー
- HP SmartアレイP841コントローラー
- HP SmartアレイP421コントローラー

HP D6000 6Gb SASディスクエンクロージャーROMフラッシュコンポーネント for VMware (esxi)

バージョン: 2.98 **(クリティカル)**
ファイル名: CP029051.md5; CP029051.zip

重要な注意！

重要: ファームウェアのアップグレードは、システムの全てのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

重要: 電源入/切シーケンスには、構成の完全性を維持することが重要です。詳細は、"HP D6000 ディスクエンクロージャーユーザーガイド"の文書を参照してください。

警告！このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注: すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/Verbose.logに記録され、フラッシュの概要は、/var/cpq/Component.logに記録されます。

事前要件

重要: ファームウェアのアップグレードは、システムの全てのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！ このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注意:すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/Verbose.logに記録され、フラッシュの概要は、/var/cpq/Component.logに記録されます。

修正

以下の問題がこのファームウェアのバージョンで修正されます:

12GB SAS HDDがエンクロージャー内に搭載されている場合、ディスクディスカバリをサポートするために、SAS エキスパンダーの設定を変更しました。

サポートしているデバイスおよび機能

HP D6000 ディスクエンクロージャーは、以下のデバイスの後部で接続できます:

- HP H222ホストバスアダプター
- HP H221ホストバスアダプター
- HP H241 Smart ホストバスアダプター
- HP SmartアレイP731mコントローラー
- HP SmartアレイP741mコントローラー
- HP SmartアレイP721mコントローラー
- HP SmartアレイP441コントローラー
- HP SmartアレイP431コントローラー
- HP SmartアレイP822コントローラー
- HP SmartアレイP841コントローラー
- HP SmartアレイP421コントローラー

HPE D6020 12 Gb SASディスクエンクロージャーROMフラッシュコンポーネント for Linux (x64)

バージョン: 2.74 **(推奨)**
ファイル名: CP036707.md5; RPMS/x86_64/firmware-d6020-2.74-1.1.x86_64.compsig; RPMS/x86_64/firmware-d6020-2.74-1.1.x86_64.rpm

重要な注意！

重要:ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。シングルドメイン構成では、ユーザーがD6020(または任意のストレージボックス)でOSをホスティングしてSEPをフラッシュすると、フラッシュ/コードロードの後でSmartComponentがSEPをリセットするため、常にハング/クラッシュします。

警告 このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/D6020.logに記録され、フラッシュの要約は、/var/cpq/Component.logに記録されます。

事前要件

重要: ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！ このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/D6020.logに記録され、フラッシュの要約は、/var/cpq/Component.logに記録されます。

サポートしているデバイスおよび機能

D6020エンクロージャーは、どのHPEストレージコントローラーとホストバスアダプターにも接続できます:

- HP SmartアレイP841コントローラー
- HP SmartアレイP441コントローラー
- HP Smart HBA H241
- HPE SmartアレイP408e-pコントローラー
- HPE SmartアレイE208e-pコントローラー
- HPE SmartアレイP408e-mコントローラー
- HP SmartアレイP741mコントローラー

HPE D6020 12 Gb SASディスクエンクロージャーROMフラッシュコンポーネントfor Windows (x64)

バージョン: 2.74 **(推奨)**
ファイル名: cp036705.compsig; cp036705.exe

重要な注意！

重要: ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。シングルドメイン構成では、ユーザーがD6020(または任意のストレージボックス)でOSをホスティングしてSEPをフラッシュすると、フラッシュ/コードロードの後でSmartComponentがSEPをリセットするため、常にハング/クラッシュします。

警告 このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:すべてのファームウェアフラッシュ進行メッセージは、%systemdrive%¥CPQSYSTEM¥Log¥D6020.logに記録され、フラッシュの要約は、%systemdrive%¥CPQSYSTEM¥Log¥cpqsetup.logに記録されます。

事前要件

重要:ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:すべてのファームウェアフラッシュ進行メッセージは、%systemdrive%¥CPQSYSTEM¥Log¥D6020.logに記録され、フラッシュの要約は、%systemdrive%¥CPQSYSTEM¥Log¥cpqsetup.logに記録されます。

サポートしているデバイスおよび機能

D6020エンクロージャーは、どのHPEストレージコントローラーとホストバスアダプターにも接続できます:

- HP Smartアレイ P841コントローラー
- HP Smartアレイ P441コントローラー
- HP Smart HBA H241
- HPE Smartアレイ P408e-pコントローラー
- HPE Smartアレイ E208e-pコントローラー
- HPE Smartアレイ P408e-mコントローラー
- HP Smartアレイ P741mコントローラー

HPE D6020 12Gb SASディスクエンクロージャーROMフラッシュコンポーネントfor VMware (ESXi)

バージョン: 2.74 **(推奨)**
ファイル名: CP036706.compsig; CP036706.md5; CP036706.zip

重要な注意！

重要:ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。シングルドメイン構成では、ユーザーがD6020(または任意のストレージボックス)でOSをホスティングしてSEPをフラッシュすると、フラッシュ/コードロードの後でSmartComponentがSEPをリセットするため、常にハング/クラッシュします。

警告 このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/D6020.logに記録され、フラッシュの要約は、/var/cpq/Component.logに記録されます。

事前要件

重要: ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！ このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/D6020.logに記録され、フラッシュの要約は、/var/cpq/Component.logに記録されます。

サポートしているデバイスおよび機能

D6020エンクロージャーは、どのHPEストレージコントローラーとホストバスアダプターにも接続できます:

- HP Smartアレイ P841コントローラー
- HP Smartアレイ P441コントローラー
- HP Smart HBA H241
- HP Smartアレイ P741mコントローラー
- HPE Smartアレイ P408e-pコントローラー
- HPE Smartアレイ E208e-pコントローラー
- HPE Smartアレイ P408e-mコントローラー

Linux (x64)向けHPE D3600/D3700/D3610/D3710 12Gb SASディスクエンクロージャーROMフラッシュコンポーネント

バージョン: 4.04 (B) **(推奨)**
ファイル名: CP037008.md5; RPMS/x86_64/firmware-d3000-4.04-2.1.x86_64.compsig; RPMS/x86_64/firmware-d3000-4.04-2.1.x86_64.rpm

重要な注意！

重要:ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。シングルドメイン構成では、ユーザーがD3000(または任意のストレージボックス)でOSをホスティングしてSEPをフラッシュすると、フラッシュ/コードロードの後でSmartComponentがSEPをリセットするため、常にハング/クラッシュします。

警告 このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:注記:すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/D3000.logに記録され、フラッシュの要約は、/var/cpq/Component.logに記録されます。

事前要件

重要:ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:注記:すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/D3000.logに記録され、フラッシュの要約は、/var/cpq/Component.logに記録されます。

サポートしているデバイスおよび機能

D3600/D3700/D3610/D3710エンクロージャーは、以下のどのHPEストレージコントローラーとホストバスアダプターにも接続できます:

- HP Smartアレイ P841コントローラー
- HP Smartアレイ P441コントローラー

- HP Smart HBA H241
- HPE SmartアレイP408e-pコントローラー
- HPE SmartアレイE208e-pコントローラー
- HPE SmartアレイP408e-mコントローラー
- HP SmartアレイP741mコントローラー

VMware (esxi)向けHPE D3600/D3700/D3610/D3710 12Gb SASディスクエンクロージャーROMフラッシュコンポーネント

バージョン: 4.04 (B) **(推奨)**
ファイル名: CP035473.compsig; CP035473.md5; CP035473.zip

重要な注意！

重要:ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。シングルドメイン構成では、ユーザーがD3000(または任意のストレージボックス)でOSをホスティングしてSEPをフラッシュすると、フラッシュ/コードロードの後でSmartComponentがSEPをリセットするため、常にハング/クラッシュします。

警告 このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:注記:すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/D3000.logに記録され、フラッシュの要約は、/var/cpq/Component.logに記録されます。

事前要件

重要:ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:注記:すべてのファームウェアフラッシュ進行メッセージは、/var/cpq/D3000.logに記録され、フラッシュの要約は、/var/cpq/Component.logに記録されます。

サポートしているデバイスおよび機能

D3600/D3700/D3610/D3710エンクロージャーは、以下のどのHPEストレージコントローラーとホストバスアダプターにも接続できます:

- HP SmartアレイP841コントローラー
- HP SmartアレイP441コントローラー
- HP Smart HBA H241
- HP SmartアレイP741mコントローラー
- HPE SmartアレイP408e-pコントローラー
- HPE SmartアレイE208e-pコントローラー
- HPE SmartアレイP408e-mコントローラー

Windows (x64)向けHPE D3600/D3700/D3610/D3710 12Gb SASディスクエンクロージャーROMフラッシュコンポーネント

バージョン: 4.04 (B) **(推奨)**
ファイル名: cp037009.compsig; cp037009.exe

重要な注意！

重要: ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。シングルドメイン構成では、ユーザーがD3000(または任意のストレージボックス)でOSをホスティングしてSEPをフラッシュすると、フラッシュ/コードロードの後でSmartComponentがSEPをリセットするため、常にハング/クラッシュします。

警告 このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:すべてのファームウェアフラッシュ進行メッセージは、%systemdrive%¥CPQSYSTEM¥Log¥D3000.logに記録され、フラッシュの要約は、%systemdrive%¥CPQSYSTEM¥Log¥cpqsetup.logに記録されます。

事前要件

重要:ファームウェアのアップグレードは、システムのすべてのI/Oを停止して、システムをメンテナンスする期間内に行う必要があります。

警告！このユニットの機能が失われる可能性があるので、ファームウェアのアップデート中は電源を切ったり再起動したりしないでください。通常ファームウェアをロードするのに数分かかります。

注記:すべてのファームウェアフラッシュ進行メッセージは、%systemdrive%¥CPQSYSTEM¥Log¥D3000.logに記録され、フラッシュの要約は、%systemdrive%¥CPQSYSTEM¥Log¥cpqsetup.logに記録されます。

サポートしているデバイスおよび機能

D3600/D3700/D3610/D3710エンクロージャーは、以下のどのHPEストレージコントローラーとホストバスアダプターにも接続できます:

- HP SmartアレイP841コントローラー
- HP SmartアレイP441コントローラー
- HP Smart HBA H241
- HPE SmartアレイP408e-pコントローラー
- HPE SmartアレイE208e-pコントローラー
- HPE SmartアレイP408e-mコントローラー
- HP SmartアレイP741mコントローラー

ソフトウェア - Lights-Outマネジメント

先頭

HP Lights-Outオンライン構成ユーティリティ for Windows x64 Editions

バージョン: 5.2.0.0 **(推奨)**
ファイル名: cp033351.compsig; cp033351.exe

重要な注意！

HPONCFG for Windows Serverでは、PRODUCTION/HIGH/FIPSセキュリティ状態のみでiLOがサポートされます。

事前要件

このユーティリティは、以下の最小ファームウェアリビジョンを必要とします。

- Integrated Lights-Out 3ファームウェアバージョン1.00以降
- Integrated Lights-Out 4ファームウェアバージョン1.00以降
- Integrated Lights-Out 5ファームウェアバージョン1.10以降

マネジメントインターフェイスドライバーがサーバーに必ずインストールされていなければなりません。

HPONCFG GUIを起動するには、Microsoft .Net Framework 2.0以降が必要です。

修正

iLOの工場出荷時デフォルト設定を行った後でIMLとIELのログがクリアされないという問題を修正しました。

拡張

iLO 5 v1.20以降のサポートを開始しました。

HP Lights-Outオンライン設定ユーティリティ for Linux (AMD64/EM64T)

バージョン: 5.3.0-0 **(オプション)**
ファイル名: hponcfg-5.3.0-0.x86_64.compsig; hponcfg-5.3.0-0.x86_64.rpm

事前要件

このユーティリティは、以下の最小ファームウェアリビジョンを必要とします。

- Integrated Lights-Out 3ファームウェアバージョン1.00以降
- Integrated Lights-Out 4ファームウェアバージョン1.00以降
- Integrated Lights-Out 5ファームウェアバージョン1.20以降

マネジメントインターフェイスドライバーおよびマネジメントエージェントはサーバーに必ずインストールされていなければなりません。

iLO 5の場合は、上記のパッケージに加え、openssl v1.0.x以降が必要です。
openssslを手動でコンパイルおよびインストールしたり、意図的に/usr/bin/openssslに再配置している場合は、PATH環境変数を設定し、正しい/意図したopenssslにHPONCFGをダイレクトする必要があります。

拡張

iLO 5 v1.20のサポートを開始しました。

HP Lights-Outオンライン設定ユーティリティ for Linux (AMD64/EM64T)

バージョン: 5.3.0-0 (A) **(オプション)**
ファイル名: hponcfg-5.3.0-0.x86_64.compsig; hponcfg-5.3.0-0.x86_64.rpm

事前要件

このユーティリティは、以下の最小ファームウェアリビジョンを必要とします。

- Integrated Lights-Out 3ファームウェアバージョン1.00以降
- Integrated Lights-Out 4ファームウェアバージョン1.00以降
- Integrated Lights-Out 5ファームウェアバージョン1.20以降

マネジメントインターフェイスドライバーおよびマネジメントエージェントはサーバーに必ずインストールされていなければなりません。

iLO 5の場合は、上記のパッケージに加え、openssl v1.0.x以降が必要です。
openssslを手動でコンパイルおよびインストールしたり、意図的に/usr/bin/openssslに再配置している場合は、PATH環境変数を設定し、正しい/意図したopenssslにHPONCFGを向ける必要があります。

拡張

iLO 5 v1.35のサポートを開始しました。

ソフトウェア - マネジメント

先頭

HPE SDK Python RPM

バージョン: 1.3.0 **(オプション)**
ファイル名: 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

修正

初期バージョン。

HPE SDK Python RPM

バージョン: 2.3.0 **(オプション)**
ファイル名: 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

拡張

最新のrpmリリース

HPE SDK Pythonモジュール

バージョン: 2.0.0 **(オプション)**
ファイル名: python-ilorest-library-2.0.0.zip

拡張

Gen10サーバーのサポート。

HPE SDK Pythonモジュール

バージョン: 2.3 **(オプション)**
ファイル名: python-ilorest-library-2.3.0.zip

拡張

- 重要なキャッシュデータをエンコード/デコードを設定する機能が追加されました。
- 増加した検証およびロード時間。

Management Bundle Smart Component for ESXi 6.0

バージョン: 2018.09.01 **(推奨)**
ファイル名: cp036328.compsig; cp036328.zip
ドライバー名およびバージョン:

拡張

- **WBEMプロバイダー**
  - Smartアレイコントローラーモデル P408-sbのサポートを追加しました
- **Agentless Management Service**
  - iLOのActive HealthログにOSの論理ディスクボリューム構成と使用率のレポートを追加

Management Bundle Smart Component for ESXi 6.5
バージョン: 2018.09.01 **(推奨)**
ファイル名: cp036329.compsig; cp036329.zip
ドライバー名およびバージョン:

拡張

- **WBEMプロバイダー**
  - Smartアレイコントローラーモデル P408-sbのサポートを追加しました
- **Agentless Management Service**
  - iLOのActive HealthログにOSの論理ディスクボリューム構成と使用率のレポートを追加

ソフトウェア - ネットワーク 先頭

HPE Intel esx-provider for VMware
バージョン: 2018.09.00 **(オプション)**
ファイル名: cp035296.compsig; cp035296.zip
ドライバー名およびバージョン:

サポートしているデバイスおよび機能

これらのドライバーは、以下のネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 361iアダプター
- HP Ethernet 1Gb 2-port 361Tアダプター
- HP Ethernet 1Gb 4-port 366FLRアダプター
- HP Ethernet 1Gb 4ポート 366Mアダプター
- HP Ethernet 1Gb 4-port 366Tアダプター
- HP Ethernet 10Gb 2-port 560FLBアダプター
- HP Ethernet 10Gb 2ポート 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2ポート 560M アダプター
- HP Ethernet 10Gb 2ポート 560SFP+ アダプター
- HP Ethernet 10Gb 2ポート 561FLR-Tアダプター
- HP Ethernet 10Gb 2-port 561Tアダプター
- HP Ethernet 10 Gb 2ポート562FLR-SFP+アダプター
- HP Ethernet 10Gb 2-port 562SFP+アダプター

HPE ProLiant Converged Network Utility for Windows Server x64 Edition
バージョン: 5.2.3.1 **(オプション)**
ファイル名: cp030269.exe

拡張

この製品は、Windows Server 2016をサポートします。

この製品は、以下のネットワークアダプターをサポートします。

- HP Flex-10 10Gb 2ポート 530Mアダプター
- HP Ethernet 10Gb 2ポート530SFP+アダプター
- HP Ethernet 10Gb 2ポート 530T ネットワークアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HP Ethernet 10Gb 2ポート557SFP+アダプター
- HPE Ethernet 4x25Gb 1ポート 620QSFP28 アダプター
- HPE Synergy 10Gb 2ポート 2820C Ethernet アダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

この製品は現在、以下のネットワークアダプターについて、 Fibre-Channel over Ethernet N-port ID Virtualization (FCoE NPIV) 構成を提供しています。

- HP Flex-10 10Gb 2ポート 530Mアダプター
- HP FlexFabric 10Gb 2ポート 533FLR-Tアダプター
- HP FlexFabric 10Gb 2ポート 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2ポート 534FLBアダプター
- HP FlexFabric 10Gb 2ポート 534Mアダプター
- HP FlexFabric 10Gb 2ポート 536FLBアダプター
- HPE FlexFabric 10Gb 4ポート 536FLR-Tアダプター
- HP FlexFabric 20Gb 2ポート 630FLBアダプター
- HP FlexFabric 20Gb 2ポート 630Mアダプター
- HP StoreFabric CN1100R デュアルポートコンバージドネットワークアダプター
- HPE StoreFabric CN1100R-Tアダプター
- HPE StoreFabric CN1200E-Tアダプター
- HPE Synergy 10Gb 2ポート 2820C コンバージドネットワークアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

この製品は現在、IPv4 Dynamic Host Configuration Protocol (DHCP)を完全にサポートしてます。

この製品は現在、 OneView 検出メカニズムを提供しています。

サポートしているデバイスおよび機能

このソフトウェアは、以下のネットワークアダプターをサポートします。

- HP Flex-10 10Gb 2-port 530Mアダプター
- HP Ethernet 10Gb 2-port 530SFP+アダプター
- HP Ethernet 10Gb 2-port 530T ネットワークアダプター
- HP FlexFabric 10Gb 2-port 533FLR-Tアダプター
- HP FlexFabric 10Gb 2-port 534FLBアダプター
- HP FlexFabric 10Gb 2-port 534FLR-SFP+アダプター
- HP FlexFabric 10Gb 2-port 534Mアダプター
- HPE FlexFabric 10Gb 4-port 536FLR-Tアダプター
- HPE FlexFabric 10Gb 2-port 556FLBアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE FlexFabric 10Gb 2-port 556FLR-Tアダプター
- HP Ethernet 10Gb 2-port 557SFP+アダプター
- HPE Ethernet 25Gb 4-port 620SFP28アダプター
- HP FlexFabric 20Gb 2-port 630FLBアダプター
- HP FlexFabric 20Gb 2-port 630Mアダプター
- HP FlexFabric 20Gb 2-port 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP StoreFabric CN1100R Dual Port Converged Network Adapter
- HPE StoreFabric CN1100R-T Dual Port Converged Network Adapter
- HPE StoreFabric CN1200E-Tアダプター
- HPE Synergy 10Gb 2820C Ethernetアダプター
- HPE Synergy 3820C 10/20Gbコンバージドネットワークアダプター

HPE ProLiantネットワークアダプター for Linux x86_64用Broadcom Active Health Systemエージェント

バージョン: 1.0.20-1 (B) **(オプション)**
ファイル名: 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

修正

SUMはこの製品をサポートしていないGen10サーバーにこの製品をインストールしようとしません。

サポートしているデバイスおよび機能

このソフトウェアは、以下のBroadcomネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2ポート 330iアダプター(22BD)
- HP Ethernet 1Gb 4ポート 331iアダプター(22BE)
- HP Ethernet 1Gb 4ポート 331FLRアダプター
- HP Ethernet 1Gb 4ポート 331Tアダプター
- HP Ethernet 1Gb 2ポート 332iアダプター(2133)
- HP Ethernet 1Gb 2ポート 332iアダプター(22E8)
- HP Ethernet 1Gb 2ポート 332Tアダプター

HPE ProLiantネットワークアダプター for Linux x86_64用Intel Active Health Systemエージェント

バージョン: 1.1.83.0-1 (B) **(オプション)**
ファイル名: 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

修正

SUMはこの製品をサポートしていないGen10サーバーにこの製品をインストールしようとしません。

サポートしているデバイスおよび機能

このソフトウェアは、以下のIntel ネットワークアダプターをサポートします。

- HP Ethernet 1Gb 2-port 361iアダプター
- HP Ethernet 1Gb 2-port 361Tアダプター
- HP Ethernet 1Gb 2-port 363iアダプター
- HP Ethernet 1Gb 2ポート 364i アダプター
- HP Ethernet 1Gb 4-port 366FLRアダプター
- HP Ethernet 1Gb 4-port 366M アダプター
- HP Ethernet 1Gb 4-port 366Tアダプター
- HP Ethernet 10Gb 2-port 560FLBアダプター
- HP Ethernet 10Gb 2-port 560FLR-SFP+ アダプター
- HP Ethernet 10Gb 2-port 560M アダプター
- HP Ethernet 10Gb 2-port 560SFP+ アダプター
- HP Ethernet 10Gb 2-port 561FLR-Tアダプター
- HP Ethernet 10Gb 2-port 561Tアダプター

ソフトウェア - ストレージコントローラー

先頭

64-bit Windows Server Editions用HPE ProLiant Smartアレイ SAS/SATA Event Notification Service

バージョン: 6.46.0.64 (D) **(オプション)**
ファイル名: cp034046.exe

拡張

Microsoft Windows 10のサポートを追加しました。

Windows Server 64ビットEditions向けHPE SmartアレイSRベント通知サービス

バージョン: 1.0.0.64 (B) **(推奨)**

ファイル名: cp034018.compsig; cp034018.exe

拡張

Microsoft Windows 10のサポートを追加しました。

ソフトウェア - ストレージファイバーチャネル

先頭

Emulex(BRCM) Fibre Channel Over Ethernet driver for VMware vSphere 6.0

バージョン: 2018.09.01 **(推奨)**
ファイル名: cp035916.compsig; cp035916.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

Updated to Driver version 12.0.1115.0

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE StoreFabric CN1200E-Tアダプター

Emulex(BRCM) Fibre Channel over Ethernet driver for VMware vSphere 6.5

バージョン: 2018.09.01 **(推奨)**
ファイル名: cp035917.compsig; cp035917.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

拡張

Updated to Driver version 12.0.1115.0

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexコンバージドネットワークアダプターでサポートされています。

XE100 シリーズ:

- HP StoreFabric CN1200E Dual Port Converged Network Adapter
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2-port 650Mアダプター
- HP FlexFabric 10Gb 2-port 556FLR-SFP+アダプター
- HPE StoreFabric CN1200E-Tアダプター

VMware vSphere 6.0用のEmulexファイバーチャネルドライバーコンポーネント

バージョン: 2018.09.01 **(推奨)**
ファイル名: cp035925.compsig; cp035925.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

修正

Fixed the following:

拡張

Driver version 11.4.329.0

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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

VMware vSphere 6.0用のQLogicファイバーチャネルドライバーコンポーネント

バージョン: 2018.09.01 **(推奨)**
ファイル名: cp035928.compsig; cp035928.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

Driver version 2.1.73.0

サポートしているデバイスおよび機能

このドライバーは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

VMware vSphere 6.5用のEmulexファイバーチャネルドライバーコンポーネント

バージョン: 2018.09.01 **(推奨)**
ファイル名: cp035926.compsig; cp035926.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

ソフトウェアリリース11.2以降は、Fibre Channel(LightPulse)アダプターおよび Converged Networkアダプター(OneConnect)に独立したソフトウェアキットが用意されています。

この変更について詳しくは、『Broadcom Software Kit Migration User Guide(Broadcomソフトウェアキット移行ユーザーガイド)』をお読みいただくことをお勧めします。

ガイドを入手するには:

1. 次へアクセスしてください:http://www.hpe.com/support/manuals
2. HPEモデル番号を使用する場合、製品の検索ボックスにアダプターのモデル番号を入力し、>>をクリックします。

このドキュメントには、FCおよびCNAアダプター用のドライバーキットを使用するための特別な手順および考慮事項が記載されています。

特別ケースでは、11.2よりも前のドライバー(オリジナル)ドライバーおよびアプリケーションが新規11.2ドライバーおよびアプリケーションに置き換えられています。また、inboxドライバーが新規11.2 out-of-box(OOB)ドライバーに置き換えられています。

修正

以下を修正しました。

- ドライバーは、リンクサービス拒否(LS_RJT)をビーコン(ネットワークプロービング)オフエントリレベルシステム(ELS) ESXオペレーティングシステムに応答します
- サーバー上で 'lpfc_nlp_slab_cnt = 32'を設定した後、ターゲットを取得できません
- XlanePriorityがゼロでない場合、xlaneset2は優先度0を設定しようとしますが、ドライバーは優先度を0の替わりにXlanePriorityに設定します。
- ドライバーパラメーターで指定されたXLanePriority値は、Small Factor Pluggable SFPおよびファイバチャネルフレームヘッダーのClass Specific Control(CS_CTL)Priorityフィールドに反映されません。

拡張

Driver version 11.4.329.0

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプターfor BladeSystem c-Class
- HP StoreFabric 84E 4-portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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

VMware vSphere 6.5用のQLogicファイバーチャネルドライバーコンポーネント

バージョン: 2018.09.01 **(推奨)**
ファイル名: cp035929.compsig; cp035929.zip
ドライバー名およびバージョン:

重要な注意！

このコンポーネントは、HPEアプリケーションによって使用されることを意図します。 これは、vmware.comおよびHPE vibsdepot.hpe.com Webページに加え、HPE特有のCPXXXX.xmlファイルから利用可能な同じドライバーを含むzipです。

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

Driver version 2.1.73.0

サポートしているデバイスおよび機能

このドライバーは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

ソフトウェア - ストレージファイバーチャネルHBA

先頭

Fibreutils for HPE Storageファイバーチャネルホストバスアダプター for Linux(x86_64)

バージョン: 3.3-5 **(オプション)**
ファイル名: fibreutils-3.3-5.x86_64.compsig; fibreutils-3.3-5.x86_64.rpm

事前要件

- 以下のパッケージをインストールする必要があります:glibc libgcc libstdc++ bash perl

拡張

一般的なアップデート。

Fibreutils for HPE Storageファイバーチャネルホストバスアダプター for Linux(x86_64)

バージョン: 3.3-5 (b) **(オプション)**
ファイル名: fibreutils-3.3-5.x86_64.compsig; fibreutils-3.3-5.x86_64.rpm

事前要件

- 以下のパッケージをインストールする必要があります:glibc libgcc libstdc++ bash perl

拡張

一般的なアップデート。

HPE Emulex Fibre Channel Enablement Kit for Red Hat Enterprise Linux 6 Server

バージョン: 11.4.334.2 **(推奨)**
ファイル名: 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

拡張

バージョン11.4.207.0にアップデートしました

HPE Emulex Fibre Channel Enablement Kit for Red Hat Enterprise Linux 7 Server

バージョン: 11.4.334.2 **(推奨)**
ファイル名: 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

重要な注意！

リリースノート:
HP StorageWorks Emulex Adapters Release Notes(英語)

拡張

バージョン11.4.207.0にアップデートしました

サポートしているデバイスおよび機能

- HP StorageWorks FC2243 4 Gb PCI-X 2.0 DC HBA
- HP FC2242SR 4Gb PCIe DCホストバスアダプター
- HP StorageWorks FC2143 4 Gb PCI-X 2.0 HBA
- HP FC2142SR 4Gb PCIeホストバスアダプター
- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP CN1000E Dual Port Converged Network Adapter
- HP CN1100E Dual Port Converged Network Adapter
- HP Ethernet 10Gb 2ポート 552M ネットワークアダプター

- HP NC553m 10Gb デュアルポート FlexFabric コンバージド ネットワークアダプター
- HP NC553iデュアルポート FlexFabric 10Gb コンバージド ネットワークアダプター
- HP NC552m デュアルポート 10Gb FlexFabric ネットワークアダプター
- HP NC552SFP 2ポート 10GbE サーバーアダプター
- HP NC551m デュアルポート FlexFabric 10Gb コンバージドネットワークアダプター
- HP NC551i デュアルポート FlexFabric 10Gb ネットワークアダプター
- HP NC550SFP デュアルポート10GbE サーバーアダプター
- HP FlexFabric 10Gb 2ポート 554M コンバージドネットワークアダプター
- HP FlexFabric 10Gb 2ポート 554FLR-SFP+ コンバージドネットワークアダプター
- HP FlexFabric 10Gb 2ポート 554FLB コンバージドネットワークアダプター
- HP NC550mデュアルポートFlex-10 10GbeマルチファンクションBL-cアダプター
- HP LPe1205A 8Gb ファイバーチャネルホストバスアダプター for BladeSystem c-Class
- Emulex LPe1205 8Gb ファイバーチャネルホストバスアダプター for c-Class BladeSystem
- Emulex LPe1105 4Gb ファイバーチャネルホストバスアダプター for c-Class BladeSystem
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP LPe1605 16Gb ファイバーチャネルホストバスアダプター for BladeSystem c-Class
- HP FlexFabric 20Gb 2ポート 650FLBアダプター
- HP FlexFabric 20Gb 2ポート 650Mアダプター
- HP FlexFabric 10Gb 2ポート 556FLR-SFP+アダプター
- HP StoreFabric CN1200E Dual Port Converged Network Adapter (FCoE)

HPE Emulex Fibre Channel Enablement Kit for SUSE Linux Enterprise Server 11 (AMD64/EM64T)

バージョン: 11.4.334.2 **(推奨)**
ファイル名: 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

拡張

バージョン11.4.207.0にアップデートしました

HPE Emulex Fibre Channel Enablement Kit for SUSE Linux Enterprise Server 12

バージョン: 11.4.334.2 **(推奨)**
ファイル名: 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

拡張

バージョン11.4.207.0にアップデートしました

HPE Emulex Smart SAN イネーブルメントキット(Linux)

バージョン: 1.0.0.0-4 (b) **(オプション)**
ファイル名: 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

重要な注意！

3PAR Smart SANユーザーガイドを取得するには、以下のリンクからStorage Information Libraryを参照してください：

Storage Information Library

(http://www.hpe.com/info/storage/docs/)

デフォルトでは、**HP 3PAR Storage** が選択されます

製品およびソリューション

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

Smart SAN機能を有効にする場合、この有効化キットのコンポーネントの前にHPEで指定されたファイバーチャネル ドライバーをインストールしなければなりません。 ドライバーは、HPE.comのウェブサイトwww.hpe.comで利用できます。

Linux FCドライバーキットfor HPE Branded Emulex FC HBAおよびメザニンカード、バージョン11.1.183.21、for RedHat 6、RedHat 7、Novell SUSE 11およびSUSE 12

ただし、Smart SAN が有効なドライバーが実行時にインストールされていない場合、ドライバーをインストールした後に、将来の使用のためにコンポーネントのイネーブルメントキットファイルを取得します。

拡張

バージョン1.0.0.0-4 (b)にアップデートしました

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric 84E 4-Portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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 イネーブルメントキット(Windows 64 ビットオペレーティングシステム)

バージョン: 1.0.0.1 (f) **(オプション)**
ファイル名: cp033240.compsig; cp033240.exe

重要な注意！

オペレーティング システムに受信トレイ ファイバ ーチャネル ドライバーのみインストールされている場合、Smart SANイネーブルメントキットは実行されません。ボックス (OOB) ファイバー チャネルドライバー以外では、Smart SAN 機能を利用する必要があります。OOB ドライバーがインストールされている場合、イネーブルメントキットでは、将来の使用のために

Smart SAN 機能が事前に有効/無効になります。OOBドライバーが有効なSmart SANがインストールされ(前提条件参照)、再起動後に有効になります。

3PAR Smart SANユーザーガイドを取得するには、以下のリンクからStorage Information Libraryを参照してください：

Storage Information Library

(http://www.hpe.com/info/storage/docs/)

デフォルトでは、**HP 3PAR Storage** が選択されます

製品およびソリューション

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

Smart SAN機能を有効にする場合、この有効化キットのコンポーネントの前にHPEで指定されたファイバーチャネル ドライバーをインストールしなければなりません。 ドライバーは、HPE.comのウェブサイトwww.hpe.comで利用できます。

HPE Storageファイバーチャネルアダプターキットfor x64 Emulex Storportドライバーv11.1.145.16 cp030886.exe

ただし、Smart SAN が有効なドライバーが実行時にインストールされていない場合、ドライバーをインストールした後に、将来の使用のためにコンポーネントのイネーブルメントキットファイルを取得します。

拡張

バージョン1.0.0.1 (f)にアップデートしました

サポートしているデバイスおよび機能

このコンポーネントは次のEmulexファイバーチャネルホストバスアダプターでサポートされています。

8Gb FC:

- HP 81E 8Gb Single Port PCIeファイバーチャネルホストバスアダプター
- HP 82E 8Gb Dual Port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric 84E 4-Portファイバーチャネルホストバスアダプター

LPe16000 (16Gb) FC:

- HP SN1000E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1000E 16Gb Single Portファイバーチャネルホストバスアダプター
- HP ファイバーチャネル16Gb LPe1605メザニン
- HP SN1100E 16Gb Dual Portファイバーチャネルホストバスアダプター
- HP SN1100E 16Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1100E 4P 16Gbファイバーチャネルホストバスアダプター
- HPE Synergy 3530C 16Gbファイバーチャネルホストバスアダプター

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

バージョン: 12.0.1107.0 **(推奨)**
ファイル名: 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

拡張

アップデートしたバージョン: 11.4.1205.0

HPE Emulex(BRCM) Fibre Channel Over Ethernet Enablement Kit for Red Hat Enterprise Linux 7 Server

バージョン: 12.0.1107.0 **(推奨)**
ファイル名: 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

拡張

アップデートしたバージョン: 11.4.1205.0

HPE Emulex(BRCM) Fibre Channel Over Ethernet Enablement Kit for SUSE Linux Enterprise Server 11 (AMD64/EM64T)

バージョン: 12.0.1107.0 **(推奨)**
ファイル名: 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

拡張

アップデートしたバージョン: 11.4.1205.0

HPE Emulex(BRCM) Fibre Channel Over Ethernet Enablement Kit for SUSE Linux Enterprise Server 12

バージョン: 12.0.1107.0 **(推奨)**
ファイル名: 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

拡張

アップデートしたバージョン: 11.4.1205.0

HPE QLogic Fibre Channel Enablement Kit for Linux

バージョン: 6.0.0.0-4 (d) **(オプション)**
ファイル名: 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

重要な注意！

リリースノート:
HPE StoreFabric QLogic アダプターリリースノート

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

バージョン6.0.0.0-4にキットをアップデートしました

サポートしているデバイスおよび機能

このバージョンのイネーブルメントキットは、以下のデバイスをサポートします:

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

HPE QLogic Fibre Channel Enablement Kit for Linux

バージョン: 6.0.0.0-4 (e) **(推奨)**
ファイル名: 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

重要な注意！

リリースノート:
HPE StoreFabric QLogic アダプターリリースノート

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

拡張

バージョン6.0.0.0-4にキットをアップデートしました

サポートしているデバイスおよび機能

このバージョンのイネーブルメントキットは、以下のデバイスをサポートします:

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA
- HP QMH2572 8Gb ファイバーチャネルホストバスアダプター for BladeSystem

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

HPE QLogic Smart SAN イネーブルメントキット (Windows) 64 ビットオペレーティングシステム

バージョン: 1.0.0.1 (e) **(オプション)**
ファイル名: cp033239.compsig; cp033239.exe

重要な注意！

オペレーティング システムに受信トレイ ファイバ ーチャネル ドライバーのみインストールされている場合、Smart SANイネーブルメントキットは実行されません。ボックス (OOB) ファイバー チャネルドライバー以外では、Smart SAN 機能を利用する必要があります。OOB ドライバーがインストールされている場合、イネーブルメントキットでは、将来の使用のために Smart SAN 機能が事前に有効/無効になります。OOBドライバーが有効なSmart SANがインストールされ(前提条件参照)、再起動後に有効になります。

3PAR Smart SANユーザーガイドを取得するには、以下のリンクからStorage Information Libraryを参照してください：

Storage Information Library

(http://www.hpe.com/info/storage/docs/)

デフォルトでは、**HP 3PAR Storage** が選択されます

製品およびソリューション

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

Smart SAN機能を有効にする場合、この有効化キットのコンポーネントの前にHPEで指定されたファイバーチャネル ドライバーをインストールしなければなりません。 ドライバーは、HPE.comのウェブサイトwww.hpe.comで利用できます。

- x64 QLogic Storport Driver v9.2.2.20用HPE Storage Fibre Channelアダプターキット、cp031252.exe
- QLogic Storport Driver for Windows Server 2012および2012 R2 v9.2.2.20用HPE Storage Fibre Channelアダプターキット、cp031253.exe
- HPE Storage Fibre Channelアダプターキット for QLogic Storportドライバー for Windows Server 2016 v9.2.2.20、cp031251.exe

ただし、Smart SAN が有効なドライバーが実行時にインストールされていない場合、ドライバーをインストールした後に、将来の使用のためにコンポーネントのイネーブルメントキットファイルを取得します。

拡張

バージョン1.0.0.1 (e)にアップデートしました

サポートしているデバイスおよび機能

このドライバーは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

HPE QLogic Smart SAN イネーブルメントキット(Linux)

バージョン: 3.3-3 (b) **(オプション)**
ファイル名: hpe-qlogic-smartsan-enablement-kit-3.3-3.x86_64.compsig; hpe-qlogic-smartsan-enablement-kit-3.3-3.x86_64.rpm

重要な注意！

3PAR Smart SANユーザーガイドを取得するには、以下のリンクからStorage Information Libraryを参照してください：

Storage Information Library

(http://www.hpe.com/info/storage/docs/)

デフォルトでは、**HP 3PAR Storage** が選択されます

製品およびソリューション

事前要件

サポートされる構成の一覧については、次のリンクから利用可能なSPOCKを参照してください:

http://www.hpe.com/storage/spock/

Smart SAN機能を有効にする場合、この有効化キットのコンポーネントの前にHPEで指定されたファイバーチャネル ドライバーをインストールしなければなりません。 ドライバーは、HPE.comのウェブサイトwww.hpe.comで利用できます。

- Red Hat Enterprise Linux 6 Server (x86-64) FCoE/FCドライバーキットfor HPE Qlogic CNA、HBAおよびメザニンHBA、バージ8.07.00.42.06.0-k1
- Red Hat Enterprise Linux 7 Server FCoE/FCドライバーキットfor HPE QLogic CNA、HBAおよびメザニンHBAおよびCNAバージョン8.07.00.42.07.0-k1
- SUSE Linux Enterprise Server 11 (AMD64/EM64T) FCoE/FCドライバーキットfor HPE Qlogic CNA、HBAおよびメザニンHBA、バージョン8.07.00.42.11.3-k

- SUSE Linux Enterprise Server 12 FCoE/FCドライバーキットfor HPE QLogic CNA、HBAおよびメザニンHBAおよびCNAバージョン 8.07.00.42.12.0-k1

ただし、Smart SAN が有効なドライバーが実行時にインストールされていない場合、ドライバーをインストールした後に、将来の使用のためにコンポーネントのイネーブルメントキットファイルを取得します。

拡張

バージョン3.3-3(b)にアップデートしました

サポートしているデバイスおよび機能

このドライバーは、以下のHPEアダプターをサポートします。

8Gb FC:

- HP 81Q PCIeファイバーチャネルホストバスアダプター
- HP 82Q 8GbデュアルポートPCIeファイバーチャネルホストバスアダプター
- HPE StoreFabric 84Q 4P 8GbファイバーチャネルHBA

16Gb FC:

- HP QMH2672 16Gb ファイバーチャネルホストバスアダプター for BladeSystem
- HP StoreFabric SN1000Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1000Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 2-port PCIeファイバーチャネルホストバスアダプター
- HP StoreFabric SN1100Q 16GB 1-port PCIeファイバーチャネルホストバスアダプター
- HPE Synergy 3830C 16G ファイバーチャネルホストバスアダプター

32Gb FC:

- HPE StoreFabric SN1600Q 32Gb Single Portファイバーチャネルホストバスアダプター
- HPE StoreFabric SN1600Q 32Gb Dual Portファイバーチャネルホストバスアダプター

ソフトウェア - システムマネジメント

先頭

Agentless Management Service (iLO 5) for Red Hat Enterprise Linux 6 Server

バージョン: 1.3.1 **(オプション)**
ファイル名: amsd-1.3.1-2954.17.rhel6.x86_64.compsig; amsd-1.3.1-2954.17.rhel6.x86_64.rpm

事前要件

- **amsdは、HPE ProLiant Gen10サーバー上のみでサポートされています。**
- **amsdは、SNMPサポートを提供しているiLO 5サービスに情報を提供します。**
- **iLO 5上でSNMP PASS-THRUを無効にし、SNMPがiLO 5上で構成されている必要があります。これらの設定を変更した後に、iLO 5のリセットが必要になることがあります。**
- **要件:**
  - 最低限必要なiLO 5ファームウェアバージョン = 1.1
  - サポートされる最小OSバージョン = Red Hat Enterprise Linux 6.9

Agentless Management Service (iLO 5) for Red Hat Enterprise Linux 7 Server

バージョン: 1.3.1 **(オプション)**

ファイル名: amsd-1.3.1-2954.23.rhel7.x86_64.compsig; amsd-1.3.1-2954.23.rhel7.x86_64.rpm

事前要件

- **amsdは、HPE Gen10サーバー上のみでサポートされています。**
- **amsdは、SNMPサポートを提供しているiLO 5サービスに情報を提供します。**
- **iLO 5上でSNMP PASS-THRUを無効にし、SNMPがiLO 5上で構成されている必要があります。これらの設定を変更した後に、iLO 5のリセットが必要になることがあります。**
- **要件:**
  - 最低限必要なiLO 5ファームウェアバージョン = 1.1
  - サポートされる最小OSバージョン = Red Hat Enterprise Linux 7.3 Errata 3.10.0.514.6.1

Agentless Management Service (iLO 5) for SUSE Linux Enterprise Server 11

バージョン: 1.3.1 **(オプション)**

ファイル名: amsd-1.3.1-2954.18.sles11.x86_64.compsig; amsd-1.3.1-2954.18.sles11.x86_64.rpm

事前要件

- **amsdは、HPE Gen10サーバー上のみでサポートされています。**
- **amsdは、SNMPサポートを提供しているiLO 5サービスに情報を提供します。**
- **iLO 5上でSNMP PASS-THRUを無効にし、SNMPがiLO 5上で構成されている必要があります。これらの設定を変更した後に、iLO 5のリセットが必要になることがあります。**
- **要件:**
  - 最低限必要なiLO 5ファームウェアバージョン = 1.1

    サポートされる最小OSバージョン = SuSE Linux Enterprise Server 11 SP4 kISO

Agentless Management Service (iLO 5) for SUSE Linux Enterprise Server 12

バージョン: 1.3.0 **(オプション)**

ファイル名: amsd-1.3.0-2804.23.sles12.x86_64.compsig; amsd-1.3.0-2804.23.sles12.x86_64.rpm

事前要件

- **amsdは、HPE Gen10サーバー上のみでサポートされています。**
- **amsdは、SNMPサポートを提供しているiLO 5サービスに情報を提供します。**
- **iLO 5上でSNMP PASS-THRUを無効にし、SNMPがiLO 5上で構成されている必要があります。これらの設定を変更した後に、iLO 5のリセットが必要になることがあります。**
- **要件:**
  - 最低限必要なiLO 5ファームウェアバージョン = 1.1
  - サポートされる最小OSバージョン = SuSE Linux Enterprise Server 12 SP2

Agentless Management Service (iLO 5) for SUSE Linux Enterprise Server 12

バージョン: 1.3.1 **(オプション)**

ファイル名: amsd-1.3.1-2954.22.sles12.x86_64.compsig; amsd-1.3.1-2954.22.sles12.x86_64.rpm

事前要件

- **amsdは、HPE Gen10サーバー上のみでサポートされています。**
- **amsdは、SNMPサポートを提供しているiLO 5サービスに情報を提供します。**
- **iLO 5上でSNMP PASS-THRUを無効にし、SNMPがiLO 5上で構成されている必要があります。これらの設定を変更した後に、iLO 5のリセットが必要になることがあります。**
- **要件:**
  - 最低限必要なiLO 5ファームウェアバージョン = 1.1
  - サポートされる最小OSバージョン = SuSE Linux Enterprise Server 12 SP2

Agentless Managementサービス for Windows X64

バージョン: 1.30.0.0 **(オプション)**
ファイル名: cp034101.compsig; cp034101.exe

重要な注意！

SMAサービスのインストールおよびイネーブルメントについて:

- インタラクティブモードでAMSをインストール中に、選択的にSMAをインストールするように求めるポップアップメッセージが表示されます。
  - ［Yes］が選択されている場合は、SMAサービスがインストールされ、実行状態に設定されます。
  - ［No］が選択されている場合は、SMAサービスがインストールされますが、サービスは有効化されません。
- サイレントモードでのAMSのインストール中に、SMAがインストールされますが、サービスは有効化されません。
- 後でSMAサービスを有効化する場合は、下記のフォルダーに移動します:%ProgramFiles%¥OEM¥AMS¥Service¥(通常は、c:¥Program Files¥OEM¥AMS¥Service)でEnableSma.bat /fを実行
- 重要:SNMPサービスコミュニティ名および権限も設定する必要があります。 これは、EnableSma.batでは実行されません。
- SMAが有効になっているときに無効化するには、下記のフォルダーに移動します:%ProgramFiles%¥OEM¥AMS¥Service¥(通常は、c:¥Program Files¥OEM¥AMS¥Service)DisableSma.bat /fを実行
- Windowsオペレーティングシステムをインストールしたあとは、すべてのMicrosoftアップデートがダウンロードおよびインストールされていることを確認してください(wuapp.exeを起動してアップデートプロセスを開始できます)。これを完了していないと、Windowsイベントログに深刻なエラー「The Agentless Management Service terminated unexpectedly.」が報告されることがあります。

AMSコントロールパネルアプレット:

- AMSコントロールパネルのアプレットUIのシステムでの表示が最適となるのは、画面解像度が1280 × 1024ピクセル以上、テキストサイズが100%のときです。

事前要件

このコンポーネントの前に、*Channel Interface Driver for Windows X64*をインストールする必要があります。

SMA(System Management Assistant)を有効化している場合は、Microsoft SNMP Serviceを有効化する必要があります。

修正

- サーバーに9つ以上のIPV6アドレスがある場合、AMSサービスは予期せず終了しなくなりました。 ただし、cpqNicIfLogMapIPV6Address OIDのみ最大9までのIPV6 アドレスを返します。
- トラップ1015,1019,1020はMIB定義と一致する正しいvarbind情報を持つようになりました。
- SMA (System Management Assistant)サービスが停止または無効になると、SMAは古いデータのSNMPクエリに応答しなくなります。

拡張

- 以下のIOデバイスのサポートを追加しました。
  - HPE Synergy 4820C 10/20/25Gb Converged Networkアダプター
  - HPE StorFabric CN1200R-T Converged Networkアダプター
  - HPE StorFabric CN1300R Converged Networkアダプター
  - HPE Synergy 6410C 25/50Gb Ethernetアダプター
  - HPE Ethernet 100Gb 1ポート 842QSFP28 アダプター
  - HPE Infiniband FDR/Ethernet 40/50Gb 2ポート547FLR-QSFPアダプター
- コントロールパネルアプレットに次の拡張機能を追加しました。
  - [SNMP]タブでは、ユーザー構成とSNMPv3の設定とともに、最大8つのトラップ送信先がサポートされています
  - iLO5の暗号化が高度なセキュリティまたはFIPSモードに設定されている場合、[SNMP]タブが正常に機能するようになりました
  - ボタンオプションを使用して、SMAサービスの開始、停止、有効化または無効化を行うことができます
  - GUIオプションを使用して時間形式を選択し、オプションの定期的なテストトラップ間隔を入力できます
  - ヘルプの内容が拡張されました
- SMA (System Management Assistant) サービスは、iLO5 FWによって生成されたすべてのMIB OIDおよびトラップをサポートするようになりました。
- Windowsイベントログにシステムシャーシクラスの IMLイベントのサポートが追加されました。
- iSCSI MIBの状態がcpqHoMibHealthStatusArrayで利用可能になります。
- AHS (Active Health System) NICリンクレコードに、Interface Descriptionの文字列が含まれるようになりました。

HPE Apollo、ProLiantおよびSynergy Gen9サーバーのHPE ProLiant Agentless Managementサービス

バージョン: 10.90.0.0 **(オプション)**
ファイル名: cp034100.exe

事前要件

このコンポーネントの前に*HPE ProLiant iLO 3/4 Channel Interface Driver for Windows X64*(バージョン3.4.0.0以降)をインストールする必要があります。

修正

- サーバーに9つ以上のIPV6アドレスがある場合、AMSサービスは予期せず終了しなくなりました。 ただし、cpqNicIfLogMapIPV6Address OIDのみ最大9までのIPV6 アドレスを返します。
- トラップ1015,1019,1020はMIB定義と一致する正しいvarbind情報を持つようになりました。

HPE ESXiオフラインバンドル for VMware vSphere 6.0
バージョン：3.3.0 **(推奨)**
ファイル名: esxi6.0uX-mgmt-bundle-3.3.0-11.zip

修正

WBEMプロバイダー

- Smartアレイプロバイダーが頻繁にバッテリ状況の変化を報告する問題を修正

Agentless Management Service

- 定期的なテストトラップ機能が無効になっている場合、OS起動時にハートビートトラップ(cpqHo2GenericTrap)送信を削除するように修正
- OS initリソースグループ内で実行されているAMSによる部分的なメモリリークの修正
- iLOストレージタブ内の表示されている内蔵SATAコントローラーにドライブが見つからないと報告する問題を修正

拡張

WBEMプロバイダー

- Smartアレイコントローラーモデル P408-sbのサポートを追加しました

Agentless Management Service

- iLOのActive Health SystemにOSの論理ディスクボリューム構成と使用率のレポートを追加 ログ

HPE ESXiオフラインバンドルfor VMware vSphere 6.5
バージョン：3.3.0 **(推奨)**
ファイル名: esxi6.5uX-mgmt-bundle-3.3.0-10.zip

修正

WBEMプロバイダー

- Smartアレイプロバイダーが頻繁にバッテリ状況の変化を報告する問題を修正

Agentless Management Service

- 定期的なテストトラップ機能が無効になっている場合、OS起動時にハートビートトラップ(cpqHo2GenericTrap)送信を削除するように修正
- OS initリソースグループ内で実行されているAMSによる部分的なメモリリークの修正
- iLOストレージタブ内の表示されている内蔵SATAコントローラーにドライブが見つからないと報告する問題を修正

拡張

WBEMプロバイダー

- Smartアレイコントローラーモデル P408-sbのサポートを追加しました

Agentless Management Service

- iLOのActive Health SystemにOSの論理ディスクボリューム構成と使用率のレポートを追加 ログ

サポートしているデバイスおよび機能

VMware vSphere バージョンサポート：

- VMware vSphere 6.5 U1
- VMware vSphere 6.5 U2

HPE ESXi ユーティリティオフラインバンドル for VMware vSphere 6.0
バージョン：3.3.0 **(推奨)**
ファイル名: esxi6.0-util-bundle-3.3.0-8.zip

重要な注意!

以下のVMware vSphere 6.0 for June 2018 用HPE VMwareユーティリティユーザーガイドを参照してください。
www.hpe.com/info/vmware/proliant-docs

拡張

Smart Storage Array Command Line Interface（SSACLI）ユーティリティがアップデートされました

HPE ESXiユーティリティオフラインバンドルfor VMware vSphere 6.5
バージョン：3.3.0 **(推奨)**
ファイル名: esxi6.5-util-bundle-3.3.0-8.zip

重要な注意!

以下のVMware vSphere 6.5 for June 2018 用HPE VMwareユーティリティユーザーガイドを参照してください。
www.hpe.com/info/vmware/proliant-docs

拡張

Smart Storage Administrator CLI (SSACLI)のアップデート

HPE Insight Management WBEM Provider for Windows Server x64 Edition

バージョン: 10.70.0.0 **(オプション)**
ファイル名: cp033066.exe

重要な注意！

バージョン10.70.0.0がGen9サーバーをサポートする最後のHPE Insight Management WBEM Providersリリースです。

事前要件

HPE Insight Management WBEM ProviderはHPE ProLiant iLO 3/4 Channel Interface とManagement Controller Drivers (バージョン3.4.0.0以降) for Windows X64がこのコンポーネントに予めインストールされていることを要求します。

また、シングル サーバーWebベースユーザーインターフェイスのためにSystem Management Homepage (SMH) コンポーネント (バージョン7.2.2.9以降) が必要です。

修正

ストレージプロバイダー(hpwmisa.dll)が原因で発生するハンドルリークを修正しました。

HPE Insightマネジメントエージェント for Windows Server x64 Edition

バージョン: 10.90.0.0 **(オプション)**
ファイル名: cp035320.exe

事前要件

HPE Insightマネジメントエージェントでは、このコンポーネントの前にWindows x64用のSNMPサービス、HPE ProLiant iLO 3/4チャネルインターフェイス、およびマネジメントコントローラードライバーがインストールされている必要があります。

また、シングル サーバーWebベースユーザーインターフェイスのためにSystem Management Homepage(SMH)コンポーネントが必要です。

HPE MegaRAID Storage Administrator StorCLI for Linux 64-bit

バージョン: 1.24.09 **(オプション)**
ファイル名: LINUX_Readme.txt; storcli-1.24.09-1.noarch.compsig; storcli-1.24.09-1.noarch.rpm

拡張

- 最初のリリース

HPE MegaRAID Storage Administrator StorCLI for VMware 6.5

バージョン: 1.24.09 **(オプション)**
ファイル名: vmware-esx-storcli-1.24.09.vib

拡張

- 最初のリリース

HPE ProLiant Agentless Management Service for Red Hat Enterprise Linux 6(AMD64/EM64T)

バージョン: 2.8.1 **(オプション)**
ファイル名: hp-ams-2.8.1-2963.13.rhel6.x86_64.rpm

事前要件

- **hp-amsは、HP ProLiant Gen8およびGen9サーバーのみでサポートされています。**
- **hp-amsは、SNMPサポートを提供しているHP iLO 4サービスに情報を提供します。**
- **HP iLO 4上でSNMPパススルーを無効にして、SNMPがHP iLO 4上で構成されている必要があります。HP iLO 4は、これらの設定を変更した後にリセットする必要がある場合があります。**
- **要件:**
  - 最低限必要なHP iLO 4ファームウェアバージョン = 1.05
  - 最低限必要なOSバージョン = Red Hat Enterprise Linux 5.6、Red Hat Enterprise Linux 6.0、SuSE Linux Enterprise Server 10 SP4、SuSE Linux Enterprise Server 11 SP1

HPE ProLiant Agentless Management Service for Red Hat Enterprise Linux 7 Server

バージョン: 2.8.1 **(オプション)**
ファイル名: hp-ams-2.8.1-2963.14.rhel7.x86_64.rpm

事前要件

- **hp-amsは、HP ProLiant Gen8およびGen9サーバーでサポートされています。**
- **hp-amsは、SNMPサポートを提供しているHP iLO 4サービスに情報を提供します。**
- **HP iLO 4上でSNMPパススルーを無効にして、SNMPがHP iLO 4上で構成されている必要があります。HP iLO 4は、これらの設定を変更した後にリセットする必要がある場合があります。**
- **要件:**
  - 最低限必要なHP iLO 4ファームウェアバージョン = 1.05
  - 最低限必要なOSバージョン = Red Hat Enterprise Linux 5.6、Red Hat Enterprise Linux 6.0、SuSE Linux Enterprise Server 10 SP4、SuSE Linux Enterprise Server 11 SP1

HPE ProLiant Agentless Management Service for SUSE LINUX Enterprise Server 11(AMD64/EM64T)

バージョン: 2.8.1 **(オプション)**
ファイル名: hp-ams-2.8.1-2963.12.sles11.x86_64.rpm

事前要件

- **hp-amsは、HP ProLiant Gen8およびGen9サーバーのみでサポートされています。**
- **hp-amsは、SNMPサポートを提供しているHP iLO 4サービスに情報を提供します。**
- **HP iLO 4上でSNMPパススルーを無効にして、SNMPがHP iLO 4上で構成されている必要があります。HP iLO 4は、これらの設定を変更した後にリセットする必要がある場合があります。**
- **要件:**

- 最低限必要なHP iLO 4ファームウェアバージョン = 1.05
- 最低限必要なOSバージョン = Red Hat Enterprise Linux 5.6、Red Hat Enterprise Linux 6.0、SuSE Linux Enterprise Server 10 SP4、SuSE Linux Enterprise Server 11 SP1

HPE ProLiant Agentless Management Service for SUSE LINUX Enterprise Server 12

バージョン: 2.8.0 **(オプション)**

ファイル名: hp-ams-2.8.0-2861.27.sles12.x86_64.compsig; hp-ams-2.8.0-2861.27.sles12.x86_64.rpm

事前要件

- **hp-amsは、HP ProLiant Gen8およびGen9サーバーでサポートされています。**
- **hp-amsは、SNMPサポートを提供しているHP iLO 4サービスに情報を提供します。**
- **HP iLO 4上でSNMPパススルーを無効にして、SNMPがHP iLO 4上で構成されている必要があります。HP iLO 4は、これらの設定を変更した後にリセットする必要がある場合があります。**
- **要件:**
  - 最低限必要なHP iLO 4ファームウェアバージョン = 1.05
  - 最低限必要なOSバージョン = Red Hat Enterprise Linux 5.6、Red Hat Enterprise Linux 6.0、SuSE Linux Enterprise Server 10 SP4、SuSE Linux Enterprise Server 11 SP1

修正

以下を修正しました。

- NIC bondingが構成されている場合に情報がhp-ams内で正しく表示されない問題に対処しました
- hp-ams内のファイバーチャネルコントローラー情報を正しく取得するために、VLANインターフェイスの優先度をEthernetインターフェイスより先にしました
- Scandirでメモリを解放する前に、適切な境界を検証するようにします

HPE ProLiant Agentless Management Service for SUSE LINUX Enterprise Server 12

バージョン: 2.8.1 **(オプション)**

ファイル名: hp-ams-2.8.1-2963.12.sles12.x86_64.rpm

事前要件

- **hp-amsは、HP ProLiant Gen8およびGen9サーバーでサポートされています。**
- **hp-amsは、SNMPサポートを提供しているHP iLO 4サービスに情報を提供します。**
- **HP iLO 4上でSNMPパススルーを無効にして、SNMPがHP iLO 4上で構成されている必要があります。HP iLO 4は、これらの設定を変更した後にリセットする必要がある場合があります。**
- **要件:**
  - 最低限必要なHP iLO 4ファームウェアバージョン = 1.05
  - 最低限必要なOSバージョン = Red Hat Enterprise Linux 5.6、Red Hat Enterprise Linux 6.0、SuSE Linux Enterprise Server 10 SP4、SuSE Linux Enterprise Server 11 SP1

HPE ProLiant Agentless Management Service for SUSE LINUX Enterprise Server 15

バージョン: 2.8.1 **(オプション)**

ファイル名: hp-ams-2.8.1-2963.18.sles15.x86_64.rpm

事前要件

- **hp-amsは、HP ProLiant Gen8およびGen9サーバーでサポートされています。**
- **hp-amsは、SNMPサポートを提供しているHP iLO 4サービスに情報を提供します。**
- **HP iLO 4上でSNMPパススルーを無効にして、SNMPがHP iLO 4上で構成されている必要があります。HP iLO 4は、これらの設定を変更した後にリセットする必要がある場合があります。**
- **要件:**
  - 最低限必要なHP iLO 4ファームウェアバージョン = 1.05

- 最低限必要なOSバージョン = Red Hat Enterprise Linux 5.6、Red Hat Enterprise Linux 6.0、SuSE Linux Enterprise Server 10 SP4、SuSE Linux Enterprise Server 11 SP1

HPE ProLiant Agentless Management Service for Windows X64

バージョン: 10.60.0.0 (C) **(オプション)**
ファイル名: cp035485.exe

事前要件

このコンポーネントの前に*HPE ProLiant iLO 3/4 Channel Interface Driver for Windows X64*(バージョン3.4.0.0以降)をインストールする必要があります。

修正

なし

HPE Smart Storage Administrator (HPE SSA) CLI for Linux 64ビット

バージョン: 3.30.14.0 **(推奨)**
ファイル名: ssacli-3.30-14.0.x86_64.compsig; ssacli-3.30-14.0.x86_64.rpm; ssacli-3.30-14.0.x86_64.txt

重要な注意！

バージョン2018.06のSPPを使用してシステムBIOSをアップデートする場合は、HPE Smart Storage Administratorをこの3.30.13.0バージョンにアップデートすることを推奨します。バージョン2018.06のSPPからBIOS構成ユーティリティで作成されたアレイは、HPE Smart Storage Administratorの古いバージョンではアクセスできません。

HPE SSACLIは従来と同様に、さらに追加の機能、能力、およびサポートされたデバイスを持ち、ご使用のストレージを構成して管理することができます。 既存のACUCLIスクリプトは、互換性を維持するために適切なバイナリまたは実行可能ファイルを呼び出すような最小限の変更のみを加える必要があります。

拡張

- 構成済みおよび未構成のドライブに対してドライブライトキャッシュを有効または無効にする機能が追加されました。

HPE Smart Storage Administrator (HPE SSA) CLI for VMware 6.0

バージョン: 3.30.14.0 **(推奨)**
ファイル名: ssacli-3.30.14.0-6.0.0.vib

重要な注意!

バージョン2018.06のSPPを使用してシステムBIOSをアップデートする場合は、HPE Smart Storage Administratorをこの3.30.13.0バージョンにアップデートすることを推奨します。バージョン2018.06のSPPからBIOS構成ユーティリティで作成されたアレイは、HPE Smart Storage Administratorの古いバージョンではアクセスできません。

拡張

- 構成済みおよび未構成のドライブに対してドライブライトキャッシュを有効または無効にする機能が追加されました。

HPE Smart Storage Administrator (HPE SSA) CLI for VMware 6.5

バージョン: 3.30.14.0 **(推奨)**
ファイル名: ssacli-3.30.14.0-6.5.0.vib

重要な注意!

バージョン2018.06のSPPを使用してシステムBIOSをアップデートする場合は、HPE Smart Storage Administratorをこの3.30.13.0バージョンにアップデートすることを推奨します。バージョン2018.06のSPPからBIOS構成ユーティリティで作成されたアレイは、HPE Smart Storage Administratorの古いバージョンではアクセスできません。

拡張

- 構成済みおよび未構成のドライブに対してドライブライトキャッシュを有効または無効にする機能が追加されました。

HPE Smart Storage Administrator (HPE SSA) CLI for Windows 64ビット

バージョン: 3.30.14.0 **(推奨)**
ファイル名: cp034622.compsig; cp034622.exe

重要な注意！

バージョン2018.06のSPPを使用してシステムBIOSをアップデートする場合は、HPE Smart Storage Administratorをこの3.30.13.0バージョンにアップデートすることを推奨します。バージョン2018.06のSPPからBIOS構成ユーティリティで作成されたアレイは、HPE Smart Storage Administratorの古いバージョンではアクセスできません。

HPE SSACLIは従来と同様に、さらに追加の機能、能力、およびサポートされたデバイスを持ち、ご使用のストレージを構成して管理することができます。 既存のACUCLIスクリプトは、互換性を維持するために適切なバイナリまたは実行可能ファイルを呼び出すような最小限の変更のみを加える必要があります。

拡張

- 構成済みおよび未構成のドライブに対してドライブライトキャッシュを有効または無効にする機能が追加されました。

HPE Smart Storage Administrator (HPE SSA) for Linux 64ビット

バージョン: 3.30.14.0 **(推奨)**
ファイル名: ssa-3.30-14.0.x86_64.compsig; ssa-3.30-14.0.x86_64.rpm; ssa-3.30-14.0.x86_64.txt

重要な注意！

バージョン2018.06のSPPを使用してシステムBIOSをアップデートする場合は、HPE Smart Storage Administratorをこの3.30.13.0バージョンにアップデートすることを推奨します。バージョン2018.06のSPPからBIOS構成ユーティリティで作成されたアレイは、HPE Smart Storage Administratorの古いバージョンではアクセスできません。

HPE SSAは既存のHPアレイコンフィギュレーションユーティリティ、またはACUのデザインをアップデートして、それらがオンラインになるのに応じて、さまざまなSmart Storageイニシアチブのために新機能と機能性を提供します。 HPE Smart Array Advanced Pack 1.0および2.0の機能は、適切なファームウェア(の使用)によりHPE SSAのベースライン機能の一部となりました。

HPE SSAは従来と同様に、さらに追加の機能、能力、およびサポートされたデバイスを持ち、ご使用のストレージを構成して管理することができます。 既存のACUスクリプトは、互換性を維持するために適切なバイナリまたは実行可能ファイルを呼び出すような最小限の変更のみを加える必要があります。

事前要件

HPE Smart Storage Administrator for Linuxは、サーバーにHPE System Management Homepageソフトウェアがインストールされている必要があります。 サーバーにHPE System Management Homepageソフトウェアがインストールされていない場合、HPE Smart Storage Administrator for Linuxをインストールする前に、HPE.comからダウンロードしてインストールしてください。

重要なアップデート: HPE SSA (GUI) for Linuxは、HPE System Management Homepageを必要とせず、実行することができます。 HPE SSAはLinux用にローカルアプリケーションモードをサポートします。 HPE System Management Homepageはサポートされていますが、HPE SSA GUIの実行には必要ありません。

起動するには、コマンドプロンプトで以下を入力してください。

ssa -local

コマンドは新しいFirefoxブラウザーウィンドウでHP SSAを開始します。ブラウザーウィンドウを閉じると、HP SSAは自動的に終了します。これは、ループバックインタ-フェイスだけに有効であって、外部のネットワーク接続には当てはまりません。

拡張

- 構成済みおよび未構成のドライブに対してドライブライトキャッシュを有効または無効にする機能が追加されました。

HPE Smart Storage Administrator (HPE SSA) for Windows 64ビット

バージョン: 3.30.14.0 **(推奨)**
ファイル名: cp034621.compsig; cp034621.exe

重要な注意！

バージョン2018.06のSPPを使用してシステムBIOSをアップデートする場合は、HPE Smart Storage Administratorをこの3.30.13.0バージョンにアップデートすることを推奨します。バージョン2018.06のSPPからBIOS構成ユーティリティで作成されたアレイは、HPE Smart Storage Administratorの古いバージョンではアクセスできません。

HPE SSAは既存のHPアレイコンフィギュレーションユーティリティ、またはACUのデザインをアップデートして、それらがオンラインになるのに応じて、様々なSmart Storageイニシアチブのために新機能と機能性を提供します。 HPE Smart Array Advanced Pack 1.0および2.0の機能は、適切なファームウェア(の使用)によりHPE SSAのベースライン機能の一部となりました。

HPE SSAは従来と同様に、さらに追加の機能、能力、およびサポートされたデバイスを持ち、ご使用のストレージを構成して管理することができます。 既存のACUスクリプトは、互換性を維持するために適切なバイナリまたは実行可能ファイルを呼び出すような最小限の変更のみを加える必要があります。

拡張

- 構成済みおよび未構成のドライブに対してドライブライトキャッシュを有効または無効にする機能が追加されました。

HPE Smart Storage Administrator Diagnostic Utility (HPE SSADU) CLI for Linux 64ビット

バージョン: 3.30.14.0 **(推奨)**
ファイル名: ssaducli-3.30-14.0.x86_64.compsig; ssaducli-3.30-14.0.x86_64.rpm; ssaducli-3.30-14.0.x86_64.txt

重要な注意！

バージョン2018.06のSPPを使用してシステムBIOSをアップデートする場合は、HPE Smart Storage Administratorをこの3.30.13.0バージョンにアップデートすることを推奨します。バージョン2018.06のSPPからBIOS構成ユーティリティで作成されたアレイは、HPE Smart Storage Administratorの古いバージョンではアクセスできません。

HPE Smart Storage Administratorの診断機能のこのスタンドアロンバージョンは、CLIからのみ利用できます。 診断レポートのGUIバージョンは、HPE Smart Storage Administrator (HPE SSA)を使用してください。

拡張

- 構成済みおよび未構成のドライブに対してドライブライトキャッシュを有効または無効にする機能が追加されました。

HPE Smart Storage Administrator Diagnostic Utility (HPE SSADU) CLI for Windows 64ビット

バージョン: 3.30.14.0 **(推奨)**

ファイル名: cp034623.compsig; cp034623.exe

重要な注意！

バージョン2018.06のSPPを使用してシステムBIOSをアップデートする場合は、HPE Smart Storage Administratorをこの3.30.13.0バージョンにアップデートすることを推奨します。バージョン2018.06のSPPからBIOS構成ユーティリティで作成されたアレイは、HPE Smart Storage Administratorの古いバージョンではアクセスできません。

HPE Smart Storage Administratorの診断機能のこのスタンドアロンバージョンは、CLIからのみ利用できます。 診断レポートのGUIバージョンは、HPE Smart Storage Administrator (HPE SSA)を使用してください。

拡張

- 構成済みおよび未構成のドライブに対してドライブライトキャッシュを有効または無効にする機能が追加されました。

HPE SNMPエージェント for Red Hat Enterprise Linux 6(AMD64/EM64T)

バージョン: 10.8.0 **(オプション)**
ファイル名: hp-snmp-agents-10.80-2965.21.rhel6.x86_64.rpm

事前要件

hp-healthおよびhp-snmp-agentsは、x86_64環境では32ビット アプリケーションとして起動します。 Linuxカーネル32ビット互換が有効にされていて(通常Linuxではデフォルト)、32ビット互換ライブラリが存在している必要があります。

hp-snmp-agentsに関連するすべてのファイルの一覧を取得するには、次のようにタイプします。

rpm -qp --requires hp-snmp-agents-<version>.rpm

HPE SNMPエージェント for Red Hat Enterprise Linux 7 Server

バージョン: 10.8.0 **(オプション)**
ファイル名: hp-snmp-agents-10.80-2965.21.rhel7.x86_64.rpm

事前要件

hp-healthおよびHP SNMPエージェント(hp-snmp-agents)は、x86_64環境では32ビットアプリケーションとして起動します。 Linuxカーネル32ビット互換が有効にされていて(通常Linuxではデフォルト)、32ビット互換ライブラリが存在している必要があります。

hp-snmp-agentsに関連するすべてのファイルの一覧を取得するには、次のように入力します:

rpm –qp ––requires hp-snmp-agents-.rpm

HPE SNMPエージェント for SUSE LINUX Enterprise Server 11(AMD64/EM64T)

バージョン: 10.8.0 **(オプション)**
ファイル名: hp-snmp-agents-10.80-2965.21.sles11.x86_64.rpm

事前要件

hp-healthおよびhp-snmp-agentsは、x86_64環境では32ビット アプリケーションとして起動します。 Linuxカーネル32ビット互換が有効にされていて(通常Linuxではデフォルト)、32ビット互換ライブラリが存在している必要があります。

hp-snmp-agentsに関連するすべてのファイルの一覧を取得するには、次のようにタイプします。

rpm -qp --requires hp-snmp-agents-<version>.rpm

HPE SNMPエージェント for SUSE Linux Enterprise Server 12

バージョン: 10.8.0 **(オプション)**
ファイル名: hp-snmp-agents-10.80-2965.22.sles12.x86_64.rpm

事前要件

hp-healthおよびHP SNMPエージェント(hp-snmp-agents)は、x86_64環境では32ビットアプリケーションとして起動します。 Linuxカーネル32ビット互換が有効にされていて(通常Linuxではデフォルト)、32ビット互換ライブラリが存在している必要があります。

hp-snmp-agentsに関連するすべてのファイルの一覧を取得するには、次のように入力します:

rpm –qp –-requires hp-snmp-agents-.rpm

HPE System Management Homepage for Linux(AMD64/EM64T)

バージョン: 7.6.3-3 **(オプション)**
ファイル名: hpsmh-7.6.3-3.x86_64.rpm

重要な注意！

SMH 7.6.0および以降のバージョンはGen 8およびGen 9サーバーのみをサポートします。将来の全てのパッチリリースはSMH webページ上でのみ行われます。HPE SMH リリースノートを参照してください。

Linux OSのユーザー用のご注意

- パスワードファイルの編集またはその他の方法により、"hpsmh"ユーザー(インストレーション中に作成)にログインアクセスを提供しないでください。
- "hpsmh"グループ(インストレーション中に作成)にユーザーを追加しないでください。

事前要件

SMHソフトウェアをインストールする前に、RPMが必要なバージョンのLinuxライブラリの依存関係が存在するかどうかを確認します。依存関係が見つからない場合、欠落した依存関係のリストが提供されます。ユーザーはRPMをインストールする前に、すべての必要な依存関係を手動でインストールして、前提条件を満たす必要があります。

拡張

次のコンポーネントをアップデートしました。

- PHPをバージョン5.6.30へ
- Zlibをバージョン1.2.11へ
- PCREをバージョン8.41へ
- Libxsltをバージョン1.1.32へ

HPE System Management Homepage for Windows x64

バージョン: 7.6.3.3 **(推奨)**
ファイル名: cp034022.exe

重要な注意！

SMH 7.6.0および以降のバージョンはGen 8およびGen 9サーバーのみをサポートします。将来の全てのパッチリリースはSMH webページ上でのみ行われます。HPE SMH リリースノートを参照してください。

拡張

次のコンポーネントをアップデートしました。

- PHPをバージョン5.6.30へ
- Zlibをバージョン1.2.11へ
- Libxsltをバージョン1.1.32へ
- PCREをバージョン8.41へ

HPE System Management Homepageテンプレート for Linux

バージョン: 10.7.0 **(オプション)**
ファイル名: hp-smh-templates-10.7.0-1485.2.noarch.rpm

事前要件

すべての依存関係がインストールされていないと、**hp-smh-templates** RPMインストールが失敗します。管理者は、このコマンドを実行することにより、必要な依存関係の一覧を検証できます。yumまたはzypperにより使用されているリポジトリにこれらの依存関係が含まれている場合は、インストールツールにより自動的に取得されます。ただし、存在しない場合は、RPMのインストールに進む前に、ユーザーが主導でインストールする必要があります。

hp-smh-templatesに関連するすべてのファイルの一覧を取得するには、次のようにタイプします。

rpm –qp –-requires hp-smh-templates-.rpm

HPE System Management Homepageテンプレート for Linux

バージョン: 10.8.0 **(オプション)**
ファイル名: hp-smh-templates-10.8.0-1486.2.noarch.rpm

事前要件

すべての依存関係がインストールされていないと、**hp-smh-templates** RPMインストールが失敗します。管理者は、このコマンドを実行することにより、必要な依存関係の一覧を検証できます。yumまたはzypperにより使用されているリポジトリにこれらの依存関係が含まれている場合は、インストールツールにより自動的に取得されます。ただし、存在しない場合は、RPMのインストールに進む前に、ユーザーが主導でインストールする必要があります。

hp-smh-templatesに関連するすべてのファイルの一覧を取得するには、次のようにタイプします。

rpm –qp –-requires hp-smh-templates-.rpm

HPEシステムヘルスアプリケーションおよびコマンドラインユーティリティ for Red Hat Enterprise Linux 6(AMD64/EM64T)

バージョン: 10.8.0 **(オプション)**
ファイル名: hp-health-10.80-1855.27.rhel6.x86_64.rpm

事前要件

hp-healthおよびhp-snmp-agentsは、x86_64環境では32ビット アプリケーションとして起動します。 Linuxカーネル32ビット互換が有効にされていて(通常Linuxではデフォルト)、32ビット互換ライブラリが存在している必要があります。

hp-healthに関連するすべてのファイルの一覧を取得するには、次のようにタイプします。

rpm -qp -requires hp-health-< version >.rpm

HPEシステムヘルスアプリケーションおよびコマンドラインユーティリティ for Red Hat Enterprise Linux 7 Server

バージョン: 10.8.0 **(オプション)**
ファイル名: hp-health-10.80-1855.21.rhel7.x86_64.rpm

事前要件

hp-healthおよびHP SNMPエージェント(hp-snmp-agents)は、x86_64環境では32ビット アプリケーションとして起動します。 Linuxカーネル32ビット互換が有効にされていて(通常Linuxではデフォルト)、32ビット互換ライブラリが存在している必要があります。

hp-healthに関連するすべてのファイルの一覧を取得するには、次のようにタイプします。

rpm –qp –requires hp-health-.rpm

HPEシステムヘルスアプリケーションおよびコマンドラインユーティリティ for SUSE LINUX Enterprise Server 11(AMD64/EM64T)

バージョン: 10.8.0 **(オプション)**
ファイル名: hp-health-10.80-1855.21.sles11.x86_64.rpm

事前要件

hp-healthおよびhp-snmp-agentsは、x86_64環境では32ビット アプリケーションとして起動します。 Linuxカーネル32ビット互換が有効にされていて(通常Linuxではデフォルト)、32ビット互換ライブラリが存在している必要があります。

hp-healthに関連するすべてのファイルの一覧を取得するには、次のようにタイプします。

rpm -qp -requires hp-health-< version >.rpm

HPEシステムヘルスアプリケーションおよびコマンドラインユーティリティ for SUSE LINUX Enterprise Server 12

バージョン: 10.8.0 **(オプション)**
ファイル名: hp-health-10.80-1855.22.sles12.x86_64.rpm

事前要件

hp-healthおよびHP SNMPエージェント(hp-snmp-agents)は、x86_64環境では32ビット アプリケーションとして起動します。 Linuxカーネル32ビット互換が有効にされていて(通常Linuxではデフォルト)、32ビット互換ライブラリが存在している必要があります。

hp-healthに関連するすべてのファイルの一覧を取得するには、次のようにタイプします。

rpm –qp –requires hp-health-.rpm

Insight Diagnosticsオンライン版 for Linux(x86-64)

バージョン: 10.60.2199 **(推奨)**
ファイル名: hpdiags-10.60.2199-2188.linux.x86_64.rpm

事前要件

HP Insight Diagnostics オンライン版 for Linuxには、以下のコンポーネントが必要です。
- HP System Management Homepage バージョン7.0.0-12以降

HP Insight Diagnostics オンライン版 for Linuxの機能を最大限に利用するために、以下のコンポーネントを推奨します。
- HP System Health Application、バージョン9.0.0以降

修正

- オンラインページのXSSの脆弱性
- libsgutils symlinkの修正

拡張

詳しくは、 Service Pack for ProLiant リリースノート を参照してください。

サポートされているサーバーの情報については、ProLiant Service Pack for ProLiant Server Support Guideを参照してください。

Insight Diagnosticsオンライン版 for Windows x64 Editions

バージョン: 10.60.2196.0 (A) **(推奨)**
ファイル名: cp034727.exe

重要な注意！

既知の制限事項:

HP Insight Diagnosticsオンライン版 for Windowsでは、Survey機能は、直接あるいはエンクロージャー経由で特定のSmartアレイコントローラー(HP Modular Smart Arrayなど)に接続されている論理ドライブのプロパティの表示をサポートしなくなりました。 影響のあるコントローラー:

- Smartアレイ6iコントローラー
- Smartアレイ641コントローラー
- Smartアレイ642コントローラー
- Smartアレイ6402コントローラー
- Smartアレイ6404コントローラー

これらのコントローラーは、論理ドライブのプロパティを入手するために使用されるコマンドをサポートしません。 現在、コントローラーにこのようなサポートとHP Insight Diagnosticsの将来のバージョンにレガシーサポートを追加する予定はありません。

回避策として、Surveyで論理ドライブのプロパティを表示するために、HP Insight Diagnosticsオンライン版 for Windowsの**8.5以前**のバージョンを使用することです。 hp.comから入手可能なHP アレイ コンフィギュレーション ユーティリティは、これらのコントローラーに接続されている論理ドライブについての情報を表示することができます。

事前要件

HP Insight Diagnostics オンライン版 for Linuxには、以下のコンポーネントが必要です。
- HP System Management Homepage バージョン7.0.0-12以降

HP Insight Diagnostics オンライン版 for Linuxの機能を最大限に利用するために、以下のコンポーネントを推奨します。
- HP ProLiant Agentless Management Serviceバージョン9.0.0.0以降
- HP ProLiant Integrated Lights-Outマネジメントインターフェイスドライバーバージョン1.15.0.0以降

拡張

P542D ストレージコントローラーのサポートを追加しました。
NVIDIA Tesla K40 XL 12Gb モジュールのサポートを追加しました。
Wellsburg 6-Port SATA Controllerのサポート
新しいGen9システムのサポート。

詳しくは、 Service Pack for ProLiant リリースノートを参照してください。

サポートされているサーバーの情報については、ProLiant Service Pack for ProLiant Server Support Guideを参照してください。

Linux 64-bit用HPE MegaRAID Storage Administrator (HPE MRSA)

バージョン: 3.91.0.0 **(オプション)**
ファイル名: 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

事前要件

.

拡張

- 最初のリリース

VMware用HPE MegaRAID Storage Administrator StorCLI

バージョン: 1.24.09 **(推奨)**
ファイル名: storcli-esxi6.5-bundle-1.24.09.zip

修正

.

VMware用HPE MegaRAID Storage Administrator StorCLI

バージョン: 1.24.09 **(オプション)**
ファイル名: storcli-esxi6.0-bundle-1.24.09.zip

修正

.

Windows 64-bit向けHPE MegaRAID Storage Administrator (HPE MRSA)

バージョン: 3.92.0.0 (B) **(オプション)**
ファイル名: cp035098.exe; cp035098_part1.compsig; cp035098_part2.compsig; cp035098_part3.compsig; cp035098_part4.compsig

---

Windows 64-bit用HPE MegaRAID Storage Administrator StorCLI

バージョン: 1.24.9.0 (B) **(オプション)**
ファイル名: cp035244.compsig; cp035244.exe

重要な注意!

- すでにファームウェアバージョン1.24.9.0をインストールしている場合、1.24.9.0(B)にアップデートする必要はありません。

拡張

- HPEデジタル署名を追加しました

Windows Server 2012 R2およびServer 2016用インテルXeon v3およびXeon v4プロセッサーでのNVMeドライブイジェクトNMIの修正

バージョン: 1.0.5.0 (B) **(オプション)**
ファイル名: cp030432.exe

拡張

サポートされるプロセッサーを示すために、コンポーネント名を変更しました。 既にバージョン1.0.5.0がインストールされたシステムはこのバージョンをインストールする必要はありません。

Windows用NVMe Drive Eject NMI Fix for Intel Xeon Processor Scalable Family

バージョン: 1.1.0.0 (B) **(オプション)**
ファイル名: cp033116.compsig; cp033116.exe

拡張

Smart Update Managerバージョン8.2.0以降で使用するときのiLO 5ノードへの展開を有効にしました。

インテグレーテッドマネジメントログビューアー for Windows Server x64 Editions

バージョン: 7.8.0.0 **(オプション)**
ファイル名: cp029435.exe

重要な注意！

バージョン7.0.0.0以降、このアプリケーションは、iLO2、iLO3、またはiLO4マネジメントコントローラーをサポートするHP ProLiantシステムにのみインストールします。 仮想マシンへのインストールはサポートされなくなりました。

バージョン6.5.0.0以降、このアプリケーションは、Windowsユーザーアカウント制御により、管理者権限が必要です。

このアプリケーションの6.2.0.0は、Windows Server 2003 x64 Editionでインストールをサポートする最後のバージョンです。

バージョン6.0.0.0から、HP ProLiantリモートモニターサービスおよびHP ProLiantリモートIMLサービスの依存性を削除しました。 このアプリケーションは、リモートシステム上でのインテグレーテッドマネジメントログへのアクセスを提供しなくなりました。

バージョン5.22.0.0以降から、このアプリケーションを32ビットと64ビットに分割したリリースが利用可能になりました。 バージョン5.21.0.0以前にダウングレードする場合は、以前の32ビットバージョンをインストールする前に、Windowsのプログラムの追加と削除を使用して64ビットリリースをアンインストールしてください。

拡張

Windows Server 2016のサポートを追加しました。
