Cisco UCS ラック サーバ ソフトウェア リリース ノート、リリース 6.0(2)

最終更新：2026 年 9 月 21 日

Cisco UCS C シリーズ サーバ

Cisco UCS C シリーズサーバは、業界標準のラック筐体でユニファイド コンピューティングの機能を提供できるため、総所有コストの軽減と俊敏性の向上に役立ちます。このシリーズの各モデルは、処理、メモリ、I/O、内蔵ストレージ リソースのバランスを取ることで、処理負荷にまつわるさまざまな課題に対応しています。

リリース ノートについて

このマニュアルでは、Cisco Integrated Management Controller（Cisco IMC）ソフトウェアおよび関連する BIOS、ファームウェア、ドライバを含む、C シリーズのソフトウェア リリース 6.0(2) の新機能、システム要件、未解決の問題、および既知の動作について説明します。このドキュメントは、関連資料 （55 ページ） セクションの一覧にあるドキュメントと併せて使用します。

（注） 元のドキュメントの発行後に、ドキュメントを更新することがあります。したがって、マニュアルのアップデートについては、Cisco.com で確認してください。

更新履歴

改定	日付	説明
C0	2026 年 6 月	次のサーバーの 6.0(2.2600xx) のリリース ノートを作成しました。 • Cisco UCS C220 M8、C240 M8、C225 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー
B0	2026 年 4 月 23 日	次のサーバーの 6.0(2.260069) のリリース ノートを作成しました。 • Cisco UCS C220 M8、C240 M8、C225 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー

改定	日付	説明
A0	2026 年 3 月 16 日	次のサーバーの 6.0(2.260044) のリリース ノートを作成しました。 • Cisco UCS C220 M8、C240 M8、C225 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー 個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェア ファイルは、次から入手可能です。Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 6.0

Cisco IMC リリース番号と .ISO イメージ名

リリース 4.3 以降、シスコでは、.ISO イメージに合わせてリリース番号の命名規則を更新しています。

例：**4.3.1.YYXXXX**

- **4.3** — メイン リリースを表します。
- **.1** — 最初のリリースを表します。

  現在の 4.3 メイン リリースの場合、**.1** は最初のリリース番号を表します。

  後続のメンテナンス リリースでは、この番号は関連するメンテナンス リリース番号を表します。
- **YY** — リリース年を表します。

  現在の 4.3 メイン リリースでは、**23** は 2023 年に由来します。
- **XXXX** — 最後の 4 桁は、毎年増加するビルド番号のシーケンスを表します。

  最初の 4.3 メイン リリースの場合、番号は **0097** です。

リリース 6.0(2) の新しいハードウェア

リリース 6.0(2.260069) の新しいハードウェア

リリース 6.0(2.260069) では、次の新しいハードウェアがサポートされています。

- NVIDIA OEM BlueField-3 B3220 DPU 2x200G QSFP112、暗号化無効（UCSC-P-N3220）（Cisco UCS C240 M7、C245 M8 および C240 M8 サーバ搭載）
- NVIDIA BlueField-3 B3220L SuperNIC 2x200G QSFP112、PCIe Gen5.0 x16、暗号無効（UCSC-P-N3220L）：Cisco UCS C240 M7、C225 M8、C245 M8、C220 M8、C240 M8 サーバー用
- Cisco UCS C220 および C240 M8 サーバで 30 TB E3.S TLC Micron 9550 ドライブをサポートします
- Cisco UCS C220 および C220 M8 サーバでの E3.S FIPS (Kioxia CM -7) ドライブのサポート

リリース 6.0(2) の新しいソフトウェア

リリース 6.0(2.260044) での新しいソフトウェア機能

次の新しいソフトウェア機能がリリース 6.0(2.260044) でサポートされています。

- mTLS クライアント CA 証明書。この機能により、サーバは認証局(CA)パブリック証明書を使用して、接続するクライアントの ID を検証できます。相互トランスポート層セキュリティ（mTLS）を使用すると、クライアントとサーバの両方が相互に認証、接続を確立する前にセキュアな双方向検証を提供します。
- SNMP 設定でのセキュア ハッシュ アルゴリズム 512（SHA 512）認証のサポート。SNMPSNMP のためのより強力で高信頼なセキュリティを実現します。
- Cisco IMC の vNIC あたり最大 9158 バイトの MTU 値の設定をサポート。この機能拡張により、Cisco UCS 15000 VIC アダプタでの高度なネットワーキングおよびストレージの使用例のジャンボ フレームのサポートが可能になります。
- Cisco IMC は、サポートされている Cisco UCS VIC アダプタの vHBA（FCイニシエータ）あたり最大 16,384 の LUN をサポートするようになりました。これにより、大規模な LUN をサポートする最新のストレージ アレイおよびホスト OS との互換性が向上します。
- RDMA 上での NFS のサポートは、 Linux 上の Cisco UCS VIC 15000 シリーズ アダプタで利用できます。
- すべての Cisco UCS VIC アダプタで、送信キュー リング サイズと受信キュー リング サイズのデフォルト値が 4096 に引き上げられました。

セキュリティ修正

リリース6.0(2.260069)でのセキュリティ修正

欠陥 ID：**CSCwr69876**

この製品には、次の Common Vulnerabilities および Exposures（CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2025-0033：AMD SEV-SNP 内の不適切なアクセス制御により、管理者特権を持つ攻撃者は SNP の初期化中に RMP に書き込みを行うことができ、SEV-SNP ゲストメモリの完全性が失われる可能性があります。
- CVE-2025-29943：AMD CPU 内での不適切な書き込み条件の処理により、管理者権限の攻撃者が CPU パイプラインの構成を変更し、SEV-SNP ゲスト内のスタック ポインタを破損する可能性があります。
- CVE-2025-48514：SEV ファームウェアでのアクセス制御の粒度が不十分であるため、権限を持つ攻撃者が SNP ゲストを攻撃するための SEV-ES ゲストを作成し、機密性を失う可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

リリース6.0(2.260044)でのセキュリティ修正

欠陥 ID：**CSCwr50426**

この製品には、次の Common Vulnerabilities および Exposures によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2024-13176：OpenSSL の ECDSA署名の計算におけるタイミング サイドチャネルの脆弱性により、ローカルアクセスまたは低遅延ネットワーク接続を持つ攻撃者が、特にNIST P-521 曲線を使用する場合に、秘密キーを回復する可能性があります。
- CVE-2024-5535：OpenSSL の SSL_select_next_proto API関数のバッファ オーバー読み取りの欠陥により、空のクライアント プロトコル バッファで呼び出される場合にトリガーされ、アプリケーションがクラッシュするか、最大 255 バイトのプライベート メモリがピアに送信される可能性があります。
- CVE-2024-9143：OpenSSL で低レベルの GF(2^m)楕円曲線 API を活用、フィールド多項式で信頼されていない明示的な値を使用すると、メモリの読み取りまたは書き込みが境界外に発生し、アプリケーションのクラッシュやリモートコード実行。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID：**CSCwr81218**

Cisco IMC には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2025-48384：Git のリンク後ろの脆弱性は、設定ファイルでの改行文字の処理に一貫性がないことに起因します。パスの末尾に改行があるサブモジュールを初期化すると、変更されたパスによって不正なチェックアウト場所が発生し、シンボリック リンクが悪意のあるフック スクリプトを指している場合、任意のコードが実行される可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID：**CSCwr83710**

Cisco IMC には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2021-0920：Linuxカーネルの Unixドメイン ソケット実装（af.unix.c の unix_scm_to_skb）の競合状態により、解放済みメモリ使用の脆弱性が発生し、ローカルの攻撃者が権限をエスカレーションしたり、システム クラッシュを引き起こしたりする可能性があります。
- CVE-2024-53150：記述子長(bLength)の不十分な検証に起因する、 Linuxカーネルの ALSA USB -audio ドライバにおける範囲外読み取りの脆弱性により、物理アクセス権を持つ攻撃者が悪意のあるUSBデバイスを使用して機密カーネルメモリの破損、またはサービス拒否の原因となります。
- CVE-2025-38352：Linuxカーネルの POSIX CPUタイマーの処理で、handle_posix_cpu_timer() および posix_cpu_timer_del() 関数との間で競合状態が発生すると、解放済みシナリオが発生し、ローカルユーザーが権限をエスカレーションしたり、システムをクラッシュさせたりする可能性があります。を参照してください。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID：**CSCws61975**

Cisco IMC には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2015-5477：ISC BIND 9 での TKEY クエリの処理エラーにより、リモートの攻撃者がエクスプロイトして REQUIRE アサーション エラーをトリガーし、指定されたデーモンを終了させ、サービス拒否を引き起こす可能性があります。
- CVE-2016-2776：ISC BIND 9 が特定のクエリに対する応答を作成する方法の欠陥により、buffer.c でアサーションが失敗する可能性があります。これにより、リモートの攻撃者が指定されたプロセスをクラッシュさせ、予期せず終了する可能性があります。

- CVE-2023-50387：「KeyTrap」として知られています。DNSSEC 検証リゾルバ（BIND や Unbound など）に存在するこの脆弱性により、リモート攻撃者が極端なCPU の枯渇とサービス拒否を引き起こす可能性があります。複雑なリソースレコードの組み合わせ。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID：**CSCws65661**

Cisco IMC には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2010-2252：Wget 1.12 以前では、-O(出力ドキュメント)オプションが使用されている場合、リモートの攻撃者が 302 リダイレクトを介して異なるファイル名を持つURLに書き込むことができます。Wget は、リダイレクトされたURLのファイル名を使用するためです。とは異なります。
- CVE-2014-4877：Wget 1.16 より前のバージョンでは、リモートFTPサーバが、再帰的取得中にディレクトリリスト内のシンボリックリンク攻撃を介して任意のファイルに書き込み、コードを実行する可能性があります。
- CVE-2016-4971：Wget 1.18 より前のバージョンでは、リモート サーバは、 HTTP 要求を FTP URL にリダイレクトすることで任意のファイルに書き込むことができます。これにより、Wget は元のHTTP ファイル名ではなく、 FTP サーバによって提供される名前でファイルを保存します。
- CVE-2017-6508：Wget 1.19.1 より前では、リモートの攻撃者が巧妙に細工されたURLを介して任意のHTTPヘッダー(CRLFインジェクション)を挿入でき、セッションハイジャックやその他のヘッダーベースの攻撃につながる可能性があります。
- CVE-2018-0494：Wget 1.19.5 より前では、リモートの攻撃者が不正な形式の Set-Cookieヘッダーを介して意図されている Cookie アクセス制限をバイパス、Cookie のインジェクションまたは上書きを引き起こす可能性があります。
- CVE-2021-31879：Wget 1.21.1 より前のバージョンでは、Content-Length などの特定のHTTP応答ヘッダーが適切に処理されないため、リモートの攻撃者がセキュリティ制御をバイパスたり、予期しない動作を引き起こしたりする可能性があります。
- CVE-2024-10524：WPS Office for Windowsの特定のバージョンにパス トラバーサルの脆弱性が存在し、攻撃者が細工されたファイルを介して任意のコードを実行できます。
- CVE-2024-38428：Wget 1.24.5 より前のバージョンには、 URIのユーザー情報を適切に解析しないという欠陥が脆弱。これがエクスプロイトされ、セキュリティ フィルタをバイパスたり、特定の設定でログイン情報が漏洩したりする可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID：CSCws68419

Cisco IMC には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2009-5155：GNU C ライブラリ（glibc）の strfmon/l 関数の off-by-one エラーにより、コンテキスト依存の攻撃者は、サービス拒否（クラッシュ）を引き起こしたり、高い精度の値を介して任意のコードを実行したりする可能性があります。
- CVE-2010-0015：GNU C ライブラリ（glibc）での NIS+ の実装により、リモートの攻撃者は、バッファ オーバーフローをトリガーする巧妙に細工された NIS+ディレクトリ名を介して、サービス拒否（クラッシュ）を引き起こしたり、任意のコードを実行したりすることが可能です。
- CVE-2011-5320：1.20.0 より前の BusyBox の tar の実装により、リモートの攻撃者は、tar ヘッダーへのディレクトリ トラバーサル攻撃を介して任意のファイルを作成または上書きできます。
- CVE-2012-4412：GNU C ライブラリ（glibc）の strcoll 関数での整数オーバーフローにより、コンテキスト依存の攻撃者は、サービス拒否（クラッシュ）を引き起こしたり、長い文字列を介して任意のコードを実行したりする可能性があります。
- CVE-2012-4424：GNU C ライブラリ（glibc）の strcoll 関数でのスタックベースのバッファ オーバーフローにより、コンテキスト依存の攻撃者は、サービス拒否（クラッシュ）を引き起こしたり、長い文字列を介して任意のコードを実行したりする可能性があります。
- CVE-2013-4237：GNU C ライブラリ（glibc）の readdir3r 関数は、特定のディレクトリ エントリを適切に処理しません。そのため、コンテキスト依存の攻撃者が、サービス拒否（境界外の読み取りとクラッシュ）を引き起こす可能性があります。
- CVE-2013-4458：GNU C ライブラリ（glibc）の getaddrinfo 関数のスタックベースのバッファ オーバーフローにより、リモートの攻撃者は多数の AF_INET6 アドレスを介してサービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2013-4788：GNU C ライブラリ（glibc）の PTR-MANGLE 実装は、ガード値を適切に初期化しないため、ローカルの攻撃者は、ポインタガード保護メカニズムをバイパスできます。
- CVE-2014-4043：2.20 より前の GNU C ライブラリ（glibc）の posix_spwnafile_actions_addopen 関数は、その path 引数をコピーしないため、コンテキスト依存の攻撃者は、解放済みメモリ使用後の脆弱性をトリガーできます。
- CVE-2014-6040：GNU C ライブラリ（glibc）の iconv 関数における範囲外の読み取りにより、コンテキスト依存の攻撃者は、巧妙に細工されたマルチバイト シーケンスを介してサービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2014-7817：GNU C ライブラリ（glibc）の wordexp 関数により、コンテキスト依存の攻撃者は、WRDE_NOCMD が指定されている場合でも、コマンド置換をトリガーする巧妙に細工された文字列を介して任意のコマンドを実行できます。

- CVE-2014-8121：GNU C ライブラリ（glibc）の nss_files 実装は、特定のデータベース ファイルを適切に処理しません。そのため、ローカルの攻撃者は、サービス拒否（無限ループ）を引き起こしたり、データベースを破損したりする可能性があります。
- CVE-2014-9402：GNU C ライブラリ（glibc）の getnetbyname 関数により、リモートの攻撃者は、巧妙に細工された DNS 応答を介して、サービス拒否（無限ループ）を引き起こすことができます。
- CVE-2014-9761：GNU C ライブラリ（glibc）の Ann 関数でのスタックベースのバッファ オーバーフローにより、コンテキスト依存の攻撃者は、長い文字列を介してサービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2015-1781：GNU C ライブラリ（glibc）の gethostbyname_r 関数におけるバッファ オーバーフローにより、コンテキスト依存の攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、長いホスト名を介して任意のコードを実行したりする可能性があります。
- CVE-2015-5180：GNU C ライブラリ（glibc）の res/query 関数における NULL ポインタの逆参照により、リモートの攻撃者は、巧妙に細工された DNS 応答を介して、サービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2015-8776：GNU C ライブラリ（glibc）の strftime 関数の範囲外アクセスにより、コンテキスト依存の攻撃者は、巧妙に細工されたフォーマット文字列を介して、サービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2015-8777：GNU C ライブラリ（glibc）の LD_PointER_GUARD 環境変数、ローカルの攻撃者は、ポインタガード保護メカニズムを無効にしてバイパスことができます。
- CVE-2015-8778：GNU C ライブラリ（glibc）の hcreate 関数の整数オーバーフローにより、コンテキスト依存の攻撃者は、多数の要素を介して、サービス拒否（クラッシュ）を生じさせることや、おそらくは任意のコードを実行することが可能になります。
- CVE-2015-8779：GNU C ライブラリ（glibc）の catopen 関数でのスタックベースのバッファ オーバーフローにより、コンテキスト依存の攻撃者は、サービス拒否（クラッシュ）を引き起こしたり、長いカタログ名を介して任意のコードを実行したりする可能性があります。
- CVE-2015-8982：GNU C ライブラリ（glibc）の strftime 関数のバッファ オーバーフローにより、コンテキスト依存の攻撃者は、巧妙に細工されたフォーマット文字列を介して、サービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2015-8983：GNU C ライブラリ（glibc）の _IO_wstr_overflow 関数の整数オーバーフローにより、コンテキスト依存の攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、大きな文字列を介して任意のコードを実行したりする可能性があります。
- CVE-2015-8984：GNU C ライブラリ（glibc）の fnmatch 関数における範囲外の読み取りにより、コンテキスト依存の攻撃者は、巧妙に細工されたパターンを介して、サービス拒否（クラッシュ）を引き起こすことができます。

- CVE-2015-8985：GNU C ライブラリ（glibc）の pop_fail_stack 関数により、コンテキスト依存の攻撃者は、拡張正規表現処理に関連するベクトルを介してサービス拒否(アサーションの失敗とクラッシュ)を引き起こすことができます。
- CVE-2016-10228：GNU C ライブラリ（glibc）の iconv 関数における範囲外の書き込みにより、コンテキスト依存の攻撃者は、巧妙に細工されたマルチバイト シーケンスを介して、サービス拒否（クラッシュ）を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2016-10739：GNU C ライブラリ（glibc）の getaddrinfo 関数のバッファオーバーフローにより、リモートの攻撃者は多数の AF_INET6 アドレスを介してサービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2016-1234：GNU C ライブラリ（glibc）の glob 関数でのスタックベースのバッファオーバーフローにより、コンテキスト依存の攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、長いパスを介して任意のコードを実行したりする可能性があります。
- CVE-2016-3075：GNU C ライブラリ（glibc）の getnetbyname 関数でのスタックベースのバッファオーバーフローにより、リモートの攻撃者は、巧妙に細工された DNS 応答を介して、サービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2016-3706：GNU C Library (glibc) の getaddrinfo 関数において、CVE-2013-4458 に対する修正が不完全であったことに起因するスタックベースのバッファオーバーフローが存在します。これにより、リモートの攻撃者は hostent 変換を伴う攻撃経路を通じて、サービス拒否（クラッシュ）を引き起こす可能性があります。
- CVE-2016-4429：GNU C ライブラリ（glibc）の clntudp_call 関数のスタックベース バッファオーバーフローにより、リモートの攻撃者は、巧妙に細工された RPC 応答を介して、サービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2017-12132：2.26 より前の GNU C ライブラリ（glibc）の DNS スタブ リゾルバは、EDNS サポートが有効になっている場合に大きな UDP 応答を要求し、 IPフラグメンテーションによるオフパス DNS スプーフィング攻撃を簡素化する可能性があります。
- CVE-2017-15670：2.27 より前の GNU C ライブラリ（glibc）の glob 関数の off-by-one エラーにより、~演算子とその後の長い文字列を使用してホーム ディレクトリを処理する際にヒープ ベースのバッファ オーバーフローが発生します。
- CVE-2017-15671：2.27 より前の GNU C ライブラリ（glibc）の glob 関数は、長いユーザー名を持つ~演算子を処理するときに割り当てられたメモリの解放をスキップし、サービス拒否(メモリ リーク)につながる可能性があります。
- CVE-2017-16997：GNU C ライブラリ（glibc）の elf/dl-load.c 実装は、特定のチェックを適切に処理しません。これにより、ローカルの攻撃者は、巧妙に細工された共有オブジェクトを介してセキュリティ制限をバイパスできます。
- CVE-2017-8804：x86_64 の GNU C ライブラリ（glibc）の memmove と memcpy の実装では、場合によっては重複するメモリ領域が適切に処理されません。これにより、コンテキスト依存の攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、影響は限定されません。

- CVE-2018-1000001：GNU C ライブラリ（glibc）の Realpath 関数のバッファ アンダーフローにより、ローカルの攻撃者は、巧妙に細工されたパスを介して、サービス拒否（クラッシュ）を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2018-11236：GNU C ライブラリ（glibc）の "vfprintf_internal 関数での整数オーバーフローにより、コンテキスト依存の攻撃者は、サービス拒否（クラッシュ）を引き起こしたり、高い精度の値を介して任意のコードを実行したりする可能性があります。
- CVE-2018-6485：GNU C ライブラリ（glibc）2.26 以前の posix_memign in memセット 関数の実装での整数オーバーフローにより、これらの関数が小さすぎるヒープ領域へのポインタを返す可能性があり、結果的にヒープにつながる可能性があります。データ破損の原因となります。
- CVE-2019-1010023：GNU C ライブラリ（glibc）の ld.soダイナミックローダーでのバッファオーバーフローにより、ローカルの攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、巧妙に細工された環境変数を介して任意のコードを実行したりする可能性があります。
- CVE-2019-19126：2.31 より前の GNU C ライブラリ（glibc）は、SUID バイナリの LD_PRELOAD環境変数を適切に処理しません。これにより、ローカルの攻撃者はセキュリティ制限をバイパスできます。
- CVE-2019-25013：EUC-KR 文字セットに変換する際の GNU C ライブラリ（glibc）の iconv 関数でのバッファ オーバーフローにより、コンテキスト依存の攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2015-8777：GNU C ライブラリ（glibc）の regcomp 関数により、コンテキスト依存の攻撃者は、巧妙に細工された正規表現を介して、サービス拒否を生じさせることや、おそらくは任意コードを実行することが可能になります。
- CVE-2020-10029：GNU C ライブラリ（glibc）の cosl 関数でのスタックベースのバッファオーバーフローにより、コンテキスト依存の攻撃者は、大きな入力値を介して、サービス拒否（クラッシュ）を生じさせることや、おそらくは任意のコードを実行することが可能になります。
- CVE-2020-1751：GNU C ライブラリ（glibc）の dl_open 関数でのスタックベースのバッファオーバーフローにより、ローカルの攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、細工された共有オブジェクトパスを介して任意のコードを実行したりする可能性があります。
- CVE-2020-1752：GNU C ライブラリ（glibc）の glob 関数の解放済み脆弱性により、コンテキスト依存の攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、巧妙に細工されたパスを介して任意のコードを実行したりする可能性があります。
- CVE-2020-27618：IBM1364 文字セットに変換する際の GNU C ライブラリ（glibc）の iconv 関数のバッファ オーバーフローにより、コンテキスト依存の攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、任意のコードを実行したりする可能性があります。

- CVE-2020-29573：GNU C ライブラリ（glibc）の printf 関数のバッファ オーバーフローにより、コンテキスト依存の攻撃者は、大きな精度の値を介してサービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2021-27645：GNU C ライブラリ（glibc）の nscd(ネーム サービスキャッシュデーモン)に存在するダブルフリーの脆弱性により、ローカルの攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2021-3326： ISO-2022-JP-3 文字セットに変換する際の GNU C ライブラリ（glibc）の iconv 関数のバッファ オーバーフローにより、コンテキスト依存の攻撃者がサービス拒否（クラッシュ）または任意のコードを実行します。
- CVE-2021-33574：GNU C ライブラリ（glibc）の mq_notify 関数における解放済みの脆弱性により、コンテキスト依存の攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、任意のコードを実行したりする可能性があります。
- CVE-2021-35942：GNU C ライブラリ（glibc）の wordexp 関数のバッファ オーバーフローにより、コンテキスト依存の攻撃者が長い文字列を介してサービス拒否（クラッシュ）を引き起こすことが可能です。
- CVE-2021-3999：GNU C ライブラリ（glibc）の getcwd 関数でのバッファ オーバーフローにより、ローカルの攻撃者が、サービス拒否（クラッシュ）を引き起こしたり、長いパスを介して任意のコードを実行したりする可能性があります。
- CVE-2022-23218：GNU C ライブラリ（glibc）の svcunix-create 関数でのスタックベースのバッファ オーバーフローにより、リモートの攻撃者は、巧妙に細工された RPC 要求を介して、サービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2022-23219：GNU C ライブラリ（glibc）の clnt_create 関数のスタックベース バッファ オーバーフローにより、リモートの攻撃者は、巧妙に細工された RPC 要求を介して、サービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2023-4527：GNU C ライブラリ（glibc）の getaddrinfo 関数のスタックベースのバッファオーバーフローにより、リモートの攻撃者は、 TCPを介して受信した大規模な DNS 応答を介してサービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2023-4806：GNU C ライブラリ（glibc）の getaddrinfo 関数の解放済み脆弱性により、リモートの攻撃者は、巧妙に細工された DNS 応答を介してサービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2023-4813：GNU C ライブラリ（glibc）の getaddrinfo 関数の解放済み脆弱性により、リモートの攻撃者は、巧妙に細工された DNS 応答を介してサービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2023-4911：GLIBC_TUNABLES環境変数の処理中に GNU C ライブラリのダイナミック ローダー ld.so でバッファオーバーフローが発生し、ローカルの攻撃者が昇格された権限で任意のコードを実行できるようになります。

- CVE-2023-5156：GNU C ライブラリ（glibc）の getaddrinfo 関数のメモリリークにより、リモートの攻撃者は、巧妙に細工された DNS 応答を介して、サービス拒否(メモリの枯渇)を引き起こすことができます。
- CVE-2024-2961： ISO-2022-CN-EXT 文字セットに変換する際の GNU C ライブラリ（glibc）の iconv 関数のバッファ オーバーフローにより、コンテキスト依存の攻撃者がサービス拒否（クラッシュ）または任意のコードを実行します。
- CVE-2024-33599：GNU C ライブラリ（glibc）の nscd（ネーム サービス キャッシュ デーモン）におけるバッファ オーバーフローにより、ローカルの攻撃者が、サービス拒否（クラッシュ）を生じさせることや、おそらくは任意のコードを実行することが可能になります。
- CVE-2024-33600：GNU C ライブラリ（glibc）の nscd（ネーム サービス キャッシュ デーモン）における NULLポインタの逆参照により、ローカルの攻撃者は、巧妙に細工された要求を介して、サービス拒否（クラッシュ）を引き起こすことができます。
- CVE-2024-33601：GNU C ライブラリ（glibc）の nscd（ネーム サービス キャッシュ デーモン）におけるバッファ オーバーフローにより、ローカルの攻撃者が、サービス拒否（クラッシュ）を生じさせることや、おそらくは任意のコードを実行することが可能になります。
- CVE-2024-33602：GNU C ライブラリ（glibc）の nscd（ネーム サービス キャッシュ デーモン）におけるバッファ オーバーフローにより、ローカルの攻撃者が、サービス拒否（クラッシュ）を生じさせることや、おそらくは任意のコードを実行することが可能になります。
- CVE-2025-0395：GNU C ライブラリ（glibc）バージョン 2.13 ~ 2.40 の assert() 関数でバッファ オーバーフローが発生します。これは、失敗メッセージに十分なスペースが割り当てられていないためで、サービス拒否につながる可能性があります。
- CVE-2025-4802：GNU C ライブラリ（glibc）バージョン 2.27 ~ 2.38 の脆弱性により、ローカルの攻撃者は、静的にコンパイルされた setuid バイナリ（dlopen のコール）内の信頼できない LD_LIBRRY_PATH を介して、悪意のある共有ライブラリをロードし、権限を昇格させることができます。
- CVE-2025-5702：GNU C ライブラリ（glibc）バージョン 2.39 以降の Power10 プロセッサ向けに最適化された strcmp 実装における脆弱性により、ベクトル レジスタが不適切に初期化され、データの破損や制御フローの変更が発生する可能性があります。
- CVE-2025-8058：GNU C ライブラリ（glibc）バージョン 2.4 ~ 2.41 の regcomp 関数での二重解放脆弱性は、メモリ割り当て障害が発生した場合にブラケット解析中に発生し、任意のコード実行を許可する可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID：CSCws68836

Cisco IMC には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2007-5116： Perl 5.8 の正規表現エンジン（regcomp.c）のポリモーフィック型ィックオプコードのサポートにおけるバッファオーバーフローにより、コンテキスト依存の攻撃者は正規表現のバイトを Unicode（UTF）文字に切り替えることで任意のコードを実行できるを参照してください。
- CVE-2008-1927： Perl 5.8.8 の Double Free 脆弱性により、コンテキスト依存の攻撃者は、UTF-8 文字を含む巧妙に細工された正規表現を使用して、サービス拒否（メモリ破損とクラッシュ）を引き起こすことができます。
- CVE-2008-5302： Perl 5.8.8 および 5.10.0 の File::Path の rmtree 関数の競合状態により、ローカル ユーザーはシンボリック リンク攻撃を介して任意の setuid バイナリを作成できます。
- CVE-2008-5303： Perl 5.8.8 の File::Path の rmtree 関数の競合状態により、ローカル ユーザーは以前のセキュリティ修正の回帰を表すシンボリック リンク攻撃を介して任意のファイルを削除できます。
- CVE-2010-1168： Perl向けの 2.25 以前の Safe（別名 Safe.pm）モジュールにより、コンテキスト依存の攻撃者は、意図されたアクセス制限をバイパス、DESTROY や AUTOLOAD などの暗黙的なメソッドを伴うベクトルを介して任意のコードを実行できます。
- CVE-2010-1447： Perlの Safe（別名 Safe.pm）モジュール 2.26 以前により、コンテキスト依存の攻撃者はアクセス制限をバイパスし、サブルート参照および遅延実行を含むベクトルを介して任意のコードを実行できます。
- CVE-2010-2761：3.50 より前の CGI.pm の multipart_init 関数は、ハードコードされたMIME 境界文字列を使用します。これにより、リモートの攻撃者は任意の HTTP ヘッダーを挿入し、 HTT P応答分割攻撃を実行できます。
- CVE-2010-4410：3.50 より前の CGI.pm のヘッダー機能における CRLF インジェクションの脆弱性により、リモートの攻撃者は任意の HTTP ヘッダーを挿入し、改行文字を介して HTTP 応答分割攻撃を実行できます。
- CVE-2011-0761： Perl 5.10.x では、コンテキスト依存の攻撃者が、getpeername、readdir、Closedir などの関数に引数を挿入することで、サービス拒否（NULL ポインタの逆参照とクラッシュ）を引き起こすことができます。
- CVE-2011-1487： Perl 5.10.x ~ 5.13.x の lc、lcfirst、uc、および ucfirst 関数は、リターン値に taint 属性を適用しないため、攻撃者は巧妙に細工された文字列を使用して汚染保護メカニズムをバイパスできます。
- CVE-2011-2939： Perlの Encode モジュールの decode_xs 関数の off-by-one エラーにより、コンテキスト依存の攻撃者は、巧妙に細工された Unicode 文字列を介してサービス拒否（メモリ破損）を引き起こしたり、任意のコードを実行したりできます。

- CVE-2011-3597： Perl の 1.17 より前のダイジェスト モジュールにおける Eval インジェクションの脆弱性により、コンテキスト依存の攻撃者が新しいコンストラクタを介して任意のコマンドを実行できる。
- CVE-2011-4116： Perlの File::Temp モジュールの _is_safe 関数がシンボリック リンクを適切に処理しないため、ローカルの攻撃者がセキュリティ チェックをバイパスできる可能性があります。
- CVE-2012-5195： Perlの Perl.Repeatcpy 関数でのヒープベースのバッファ オーバーフローにより、コンテキスト依存の攻撃者がサービス拒否を引き起こしたり、「x」文字列のリピート演算子を介して任意のコードを実行したりできるようになります。
- CVE-2012-5526： Perlの 3.63 より前の CGI.pm は、Set-Cookie または P3P ヘッダーの改行を適切にエスケープしないため、リモートの攻撃者が任意のヘッダーをHTTP応答に挿入できます。
- CVE-2012-6329： Perl 5.17.7 より前の Locale::Maketext の実装では、バックスラッシュとメソッド名が適切に処理されないため、コンテキスト依存の攻撃者は、巧妙に細工された変換文字列を介して任意のコマンドを実行できます。
- CVE-2013-1667： Perl 5.8.2 ~ 5.16.x の再ハッシュメカニズムにより、コンテキスト依存の攻撃者は、巧妙に細工されたハッシュキーを介してサービス拒否（メモリ消費とクラッシュ）を引き起こすことができます。
- CVE-2013-7422： Perl 5.20 より前の正規表現エンジン（regcomp.c）の整数アンダーフローにより、コンテキスト依存の攻撃者が任意のコードを実行したり、長い桁列を介してサービス拒否を引き起こしたりできるようになります。
- CVE-2014-4330：2.154 より前の Data::Dumper の Dumper メソッドにより、コンテキスト依存の攻撃者が、深くネストされた Array-Referenceを介してサービス拒否(スタックの枯渇とクラッシュ)を引き起こす可能性があります。
- CVE-2015-8853： Perl 5.24.0 より前の正規表現エンジンでは、コンテキスト依存の攻撃者が、巧妙に細工された UTF-8 データを介してサービス拒否（無限ループと高いCPU使用率）を引き起こすことができます。
- CVE-2016-1238： Perl 5.x(5.22.3 および 5.24.1 より前)は、モジュール包含パス(ATINC)から現在のディレクトリ(「.」)を適切に削除せず、ローカルユーザーがトロイの木馬モジュールを介して権限を取得できるようになります。
- CVE-2016-2381： Perl は、コンテキスト依存の攻撃者が、envp 配列の重複環境変数を使用し、子プロセスの汚染保護メカニズムをバイパス可能性があります。
- CVE-2016-6185： Perlの XSLoader::load メソッドは、文字列 eval で呼び出されたときに共有オブジェクト（.so）ファイルを適切に検索しないため、ローカル ユーザーが悪意のあるライブラリを介して任意のコードを実行する可能性があります。
- CVE-2018-12015： Perl 5.26.2 までの Archive::Tar モジュールにより、リモートの攻撃者はディレクトリトラバーサル保護をバイパスし、シンボリックリンクと同じ名前の通常のファイルを含むアーカイブを介して任意のファイルを上書き。

- CVE-2018-18311 ：Perl 5.26.3 および 5.28.1 より前には、無効な書き込み操作をトリガーする巧妙に細工された正規表現を介したバッファ オーバーフローの脆弱性があります。
- CVE-2018-6913： Perl 5.26.2 より前のパック関数のヒープベースのバッファ オーバーフローにより、コンテキスト依存の攻撃者が大量の項目数を介して任意のコードを実行できるようになります。
- CVE-2020-10543 ：Perl 5.30.3 より前の 32 ビット プラットフォームでは、ネストされた正規表現修飾子に整数オーバーフローがあるため、ヒープベースのバッファ オーバーフローが発生します。
- CVE-2020-10878 - 5.30.3 より前のPerlには、正規表現エンジンでの特定の命令の誤った処理に関連する整数オーバーフローがあり、命令インジェクションにつながる可能性があります。
- CVE-2020-12723： Perl 5.30.3 より前の正規表現コンパイラ(regcomp.c)のバッファ オーバーフローの脆弱性が、S_study_chunk の再帰的コール中に発生します。
- CVE-2020-16156：CPAN 2.28 では、署名検証バイパスが可能です。これにより、攻撃者は、ネットワークからダウンロードしたPerlモジュールのセキュリティ チェックをバイパスできる可能性があります。
- CVE-2023-31484：CPAN.pm（2.35 より前）およびPerl（5.38.0より前）は、 HTTPS を介してディストリビューションをダウンロードするときにTLS証明書を検証しないため、ユーザーが中間者攻撃にさらされます。
- CVE-2023-47038：不正なUnicodeプロパティを使用して巧妙に細工された正規表現をコンパイルする場合に、 Perl 5.30.0 ~ 5.38.0 でヒープ ベースのバッファ オーバーフローの脆弱性が見つかりました。
- CVE-2024-56406：Perl の tr 演算子におけるヒープ バッファ オーバーフローの脆弱性は、非ASCIIバイトを処理する際に発生し、サービス拒否や任意のコード実行につながる可能性があります。
- CVE-2025-40909：ディレクトリハンドルの複製中にPerlスレッドの競合状態が発生すると、現在の作業ディレクトリが予期せず変更され、ローカルの攻撃者がスレッドを誘導して悪意のあるコードをロードする可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID：**CSCwr84274**

Cisco IMC には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2025-27363：FreeTypeバージョン2.13.0以前の境界外書き込みの脆弱性は、TrueType GX および可変フォント ファイルのフォント サブグラフ構造を解析するときに発生しま

す。不適切なデータ型の割り当ては、バッファのラップアラウンドとヒープ割り当ての上限につながり、任意のコード実行を許可する可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID：CSCwr84317

Cisco IMC には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2023-38545：curl の SOCKS5プロキシハンドシェイクにおけるシビラティ（重大度）の高いヒープベースのバッファ オーバーフローの脆弱性は、低速なハンドシェイク中に 255 バイトを超えるホスト名がターゲット バッファに誤ってコピーされた場合に発生し、悪意のあるプロキシがクライアントで任意のコードを実行できる可能性があります。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

不具合 ID - CSCwq11344

Cisco IMC には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-1999-0289：Win32 用のApache Web サーバは、要求されたURLにドット（.）が付加されている場合、制限されたファイルへのアクセスを提供する可能性があり、不正なファイル開示を許可する可能性があります。
- CVE-1999-0678：Debian GNU/ Linux 上の Apache のデフォルト設定では、ServerRoot が /usr/doc に設定されます。これにより、リモート ユーザーはサーバ全体のドキュメント ファイルを読み取ることができます。
- CVE-2010-1151： Apache HTTP サーバの mod_auth_shadow モジュールの競合状態により、リモートの攻撃者は認証をバイパス、外部ヘルパー アプリケーションとの不適切な対話によってデータを読み取りまたは変更することができます。
- CVE-2023-31122： Apache HTTPサーバ バージョン 2.4.57 までの mod_macro モジュールにおける範囲外の読み取りの脆弱性により、攻撃者が長いマクロの処理時にクラッシュを引き起こしたり、機密情報を取得したりする可能性があります。
- CVE-2023-38709：バージョン 2.4.58 までのApache HTTPサーバのコアにおける入力検証の失敗により、悪意のある、またはエクスプロイト可能なバックエンドコンテンツ ジェネレータがHTTP応答を分割し、キャッシュポイズニングや XSS につながる可能性があります。
- CVE-2023-43622：mod_http2 モジュールの欠陥により、攻撃者は初期ウィンドウ サイズが 0 でHTTP/2 接続を開き、その接続の処理を無期限にブロックし、「slow loris」形式の攻撃でワーカー リソースを使い果たします。

- CVE-2023-45802：クライアントによってHTTP/2ストリームがリセットされても、メモリリソースがすぐに再要求されないことがあります。これにより、クライアントは、サーバのメモリ フットプリントを増加させ、サービス拒否を引き起こす可能性があります。
- CVE-2024-24795：複数のApache HTTPサーバーモジュールに存在するHTTP応答分割の脆弱性により、攻撃者は悪意のある応答ヘッダーをバックエンド アプリケーションに挿入し、結果としてHTTP 非同期攻撃を引き起こします。
- CVE-2024-27316： Apache HTTP サーバが、単一ストリーム内で送信される HTTP/2 CONTINATIONフレームの量を制限できません。これにより、メモリが枯渇し、サービス妨害状態が発生する可能性があります。
- CVE-2024-36387： Apache HTTP サーバでHTTP /2 接続を介して WebSocket プロトコルのアップグレードを提供すると、Null ポインタの逆参照が発生し、サーバー プロセスがクラッシュする可能性があります。
- CVE-2024-38472： WindowsのApache HTTP Server における Server-Sside Request Forgery（SSRF）の脆弱性により、攻撃者は巧妙に細工されたリクエストまたはコンテンツを介して悪意のあるサーバに NTLM ハッシュをリークする可能性があります。
- CVE-2024-38473：mod_proxy モジュールでのエンコーディングの問題により、エンコーディングが正しくない要求 URL がバックエンド サービスに送信され、巧妙に細工された要求を介して認証をバイパスする可能性があります。
- CVE-2024-38474：mod_rewrite における置換エンコーディングの問題により、攻撃者は、設定によって許可されているが、URLによって直接到達できないディレクトリでスクリプトを実行したり、CGI の実行のみを目的としたスクリプト ソース コードを開示したりできます。
- CVE-2024-38475：mod_rewrite での出力のエスケープが不適切なため、攻撃者は、提供は許可されているが直接到達することを意図していないファイル システムの場所に URL をマッピングし、コードが実行される可能性があります。
- CVE-2024-38476： Apache HTTPサーバーのコアにおける脆弱性により、悪意のある応答ヘッダーまたはエクスプロイト可能なバックエンドアプリケーションを介した情報漏洩、SSRF、またはローカル スクリプトの実行が可能になります。
- CVE-2024-38477： Apache HTTP サーバーの mod_proxy モジュールにおける nullポインタの逆参照により、攻撃者は細工された悪意のあるリクエストを介してサーバーをクラッシュさせることができます。
- CVE-2024-39573：mod_rewrite における SSRF の潜在的な脆弱性により、攻撃者は安全でない RewriteRules を引き起こし、mod-proxy によって処理される URL を予期せず設定し、意図されたアクセス制御をバイパスする可能性があります。
- CVE-2024-40898：サーバ/vhost コンテキストでの mod-rewrite を伴う Windows 上の ApacheHTTP サーバにおける SSRF の脆弱性により、巧妙に細工された要求を介して悪意のあるサーバに NTLM ハッシュを漏洩する可能性があります。

- CVE-2025-3891： Apache HTTP サーバの mod_auth_openidc モジュールの欠陥により、リモートの攻撃者は、OIDCPPreservePostディレクティブが有効になっている場合に空のPOSTリクエストを送信して、サービス拒否をトリガーできます。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

欠陥 ID：CSCws68830

Cisco IMC には、次の Common Vulnerabilities および Exposures （CVE）によって識別される脆弱性の影響を受けるサードパーティ ソフトウェアが含まれています。

- CVE-2005-3962： Perl 5.8.6 および 5.9.2 のフォーマット文字列機能（Perl_sv_vcatpvfn）の整数オーバーフローにより、攻撃者は任意のメモリを上書きたり、大きな値を持つフォーマット文字列指定子を介して任意のコードを実行したりできます。
- CVE-2005-4278：Gentoo Linux上の 5.8.7-r1 より前のPerlにおける信頼できない検索パスの脆弱性により、Portage グループ内のローカル ユーザーが Portage の一時的なビルドディレクトリ内の悪意のある共有オブジェクトを介して権限を取得する可能性があります。
- CVE-2007-5116： Perl 5.8 の正規表現エンジン(regcomp.c)のポリモーフィック型オプコードのサポートにおけるバッファオーバーフローにより、コンテキスト依存の攻撃者は正規表現のバイトを Unicode 文字に切り替えて任意のコードを実行できます。
- CVE-2010-1158： Perl 5.8.x の正規表現エンジンの整数オーバーフローにより、コンテキスト依存の攻撃者は、巧妙に細工された正規表現を長い文字列と照合することで、サービス拒否（スタック消費とクラッシュ）を引き起こすことができます。
- CVE-2011-2728：5.14.2 より前の Perlの File::Glob モジュールの bsd_glob 関数により、コンテキスト依存の攻撃者は GLOB_ALTDIRFUNC フラグを使用した glob 式を介してサービス拒否（クラッシュ）を引き起こし、初期化されていないポインタの逆参照をトリガーできます。
- CVE-2011-2939： Perlの Encode モジュールの decode_xs 関数の off-by-one エラーにより、コンテキスト依存の攻撃者は、巧妙に細工された Unicode 文字列を介してサービス拒否（メモリ破損）を引き起こしたり、任意のコードを実行したりできます。
- CVE-2012-6329： Perl 5.17.7 より前の Locale::Maketext の実装では、バックスラッシュとメソッド名が適切に処理されないため、コンテキスト依存の攻撃者は、巧妙に細工された変換文字列を介して任意のコマンドを実行できます。
- CVE-2013-1667： Perl 5.8.2 ~ 5.16.x の再ハッシュメカニズムにより、コンテキスト依存の攻撃者は、巧妙に細工されたハッシュキーを介してサービス拒否（メモリ消費とクラッシュ）を引き起こすことができます。
- CVE-2014-4330：2.154 より前の Data::Dumper の Dumper メソッドにより、コンテキスト依存の攻撃者が、深くネストされた Array-Referenceを介してサービス拒否(スタックの枯渇とクラッシュ)を引き起こす可能性があります。

- CVE-2015-8853： Perl 5.24.0 より前の正規表現エンジンでは、コンテキスト依存の攻撃者が、巧妙に細工された UTF-8 データを介してサービス拒否（無限ループと高いCPU使用率）を引き起こすことができます。
- CVE-2016-1238： Perl 5.x(5.22.3 および 5.24.1 より前)は、モジュール包含パス(ATINC)から現在のディレクトリ(「.」)を適切に削除せず、ローカルユーザーがトロイの木馬モジュールを介して権限を取得できるようになります。
- CVE-2016-2381： Perl は、コンテキスト依存の攻撃者が、envp 配列の重複環境変数を使用し、子プロセスの汚染保護メカニズムをバイパス可能性があります。
- CVE-2017-12814： Windows の 5.24.3-RC1 より前の Perl および 5.26.1-RC1 より前の 5.26.x の Win32/perlhost.h の CPerlHost::Add メソッドで、攻撃者が任意の長い環境変数を介した任意のコードの。
- CVE-2017-12837： Perl 5.24.3-RC1 未満および 5.26.1-RC1 未満の 5.26.x 系における regcomp.c 内の S_regatom 関数には、ヒープベースのバッファオーバーフローの脆弱性が存在します。この脆弱性を悪用されると、リモートの攻撃者が、\N{} エスケープと大文字・小文字を区別しない（case-insensitive）修飾子を含む正規表現を用いて、サービス拒否（DoS）状態を引き起こす可能性があります。
- CVE-2017-12883： Perl 5.24.3-RC1 および 5.26.1（5.26.1-RC1 より前の 5.26.x）の regcomp.c の S_grok_bslash_N 関数のバッファ オーバーフローにより、リモートの攻撃者が機密情報を開示したり、無効な \N{U+...} エスケープを含む巧妙に細工された正規表現。
- CVE-2018-12015： Perl 5.26.2 までの Archive::Tar モジュールにより、リモートの攻撃者はディレクトリトラバーサル保護をバイパスし、シンボリックリンクと同じ名前の通常のファイルを含むアーカイブを介して任意のファイルを上書き。
- CVE-2018-18311： Perl 5.26.3 および 5.28.1 より前のPerl_my_setenv 関数の整数オーバーフローにより、ローカルの攻撃者がサービス拒否を引き起こしたり、大きな環境変数を介して任意のコードを実行したりできる。
- CVE-2018-18312： Perl 5.26.3 および 5.28.1 より前の regcomp.c の S_handle_regex_sets 関数におけるヒープ ベースのバッファ オーバーフローにより、リモートの攻撃者がサービス拒否を引き起こしたり、巧妙に細工された正規表現を介して任意のコードを実行したりできるようになります。
- CVE-2018-18313： Perl 5.26.3 および 5.28.1 より前の regcomp.c の S_grok_bslash_N 関数によるヒープベースのバッファ読み取りオーバーフローにより、リモート攻撃者が巧妙に細工された正規表現を介してプロセス メモリから機密情報を開示できるようになります。
- CVE-2018-18314： Perl 5.26.3 および 5.28.1 より前の regcomp.c の S_regtom 関数でのヒープベースのバッファ オーバーフローにより、リモートの攻撃者がサービス拒否を引き起こしたり、巧妙に細工された正規表現を介して任意のコードを実行したりできるようになります。
- CVE-2018-6913： Perl 5.26.2 より前のパック関数のヒープベースのバッファ オーバーフローにより、コンテキスト依存の攻撃者が大量の項目数を介して任意のコードを実行できるようになります。

- CVE-2020-10543 ：Perl 5.30.3 より前の 32 ビット プラットフォームでは、ネストされた正規表現修飾子に整数オーバーフローがあるため、ヒープベースのバッファ オーバーフローが発生します。
- CVE-2020-10878 - 5.30.3 より前のPerlには、正規表現エンジンでの特定の命令の誤った処理に関連する整数オーバーフローがあり、命令インジェクションにつながる可能性があります。
- CVE-2020-12723： Perl 5.30.3 より前の正規表現コンパイラ(regcomp.c)のバッファ オーバーフローの脆弱性が、S_study_chunk の再帰的コール中に発生します。
- CVE-2022-48522：警告メッセージを出力しようとすると、 Perl 5.34.var 関数のスタックベースのクラッシュ(無限再帰)が発生し、サービス拒否につながる可能性があります。
- CVE-2023-31484：CPAN.pm（2.35 より前）およびPerl（5.38.0より前）は、 HTTPS を介してディストリビューションをダウンロードするときにTLS証明書を検証しないため、ユーザーが中間者攻撃にさらされます。
- CVE-2023-31486： Perlコア モジュールであるHTTP ：0.083 より前の には、安全でないデフォルトTLS設定があり、ユーザーが証明書の検証をオプトインする必要があり、アプリケーションが中間者攻撃にさらされる可能性があります。
- CVE-2023-47039： Perl for Windowsのバイナリハイジャックの脆弱性は、システムパスに依存してシェル(cmd.exe)を見つけ、まず現在の作業ディレクトリを検索して、ローカル特権昇格を許可するために発生します。

影響を受けるサードパーティ ソフトウェア コンポーネントを脆弱性の修正が含まれるバージョンにアップグレードする必要があります。製品の今後のバージョンはこの脆弱性の影響を受けません。

解決済みの不具合

リリースで解決済みの問題 6.0(2.2600xx)

リリース 6.0(2.2600xx) では、次の問題が解決されました。

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCwn42410	RAID 1 ペアの 1 つの M.2 ドライブが部分的に応答しなくなり、ドライブが空のように見え、リンク速度が低下し、ストレージ障害が動作不能または劣化したことが報告される場合があります。 この問題は、 RAID 1 で構成された M.2 ドライブで Cisco UCS M.2 ハードウェア RAID コントローラを使用するサーバに影響します。 この問題は解決されました。	4.3(2.230207)	6.0(2.2600xx)
CSCwt65289	ホストファームウェアのアップグレード中に、Samsung PM1743 または PM1745 NVMe ドライブを搭載したサーバは、アップグレードが成功し、ドライブが正常に動作している場合でも、一時的に動作不能障害を報告することがあります。 これは、PM1743 または PM1745 NVMe ドライブを搭載した Cisco UCS C シリーズのサーバで、特にアップグレード後にホストが再起動する場合に見られました。 この問題は解決されました。	6.0(2.260044)	6.0(2.2600xx)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済みリリース
CSCwt96184	PCI 処理の問題により、影響を受ける Cisco UCS VIC アダプタで PCI バス エラーによりゲスト オペレーティング システムがクラッシュ トリガー可能性があります。 この問題は、 ESXi 8.0 U3 を使用する環境を含む Cisco UCS VIC 14xx アダプタで観察されています。 この問題は解決されました。	4.3(6.260023)	6.0(2.260069)
CSCws60510	LDAP セキュア ポートがデフォルト以外のポートに設定されている場合、LDAP セキュア認証で誤った検索フィルタが使用され、ディレクトリのルックアップが失敗する場合があります。 これは、LDAP セキュアが 636 以外のポートを使用した場合に Cisco UCS C225 M8 サーバで発生します。 この問題は解決されました。	6.0(1.250174)	6.0(2.260069)

リリースで解決済みの問題 6.0(2.260069)

リリース 6.0(2.260069) では、次の問題が解決されました。

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCwb34870	ファームウェアバージョン 6.0.2.260044 を実行している Cisco UCS C シリーズ サーバでは、プライベート企業OID で `snmpget` 操作を実行すると、簡易網管理プロトコル（SNMP）サービスがハングし、その後 `snmpwalk` 要求が失敗する場合があります。サービスが応答しなくなった場合は、ベースボード管理コントローラ（BMC）を再起動するか、SNMP サービスを無効にして再度有効にすることでサービスを復元できます。 この問題は解決されました。	6.0(2.260044)	6.0(2.260069)
CSCwt18924	VIC 1467 アダプタを搭載した Cisco UCS C220 M6 サーバでは、アップストリーム ACI スイッチをアップグレードして再起動すると、メモリ不足エラーによる致命的なクラッシュが発生します。物理インターフェイスは起動しますが、vNIC は初期化状態のままになり、自動的に回復しません。アダプタログには、致命的なエラーからのリセットが示されます。 この問題は解決されました。	4.3(5.250030)	6.0(2.260069)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済みリリース
CSCwb35920	スペアとして出荷された特定の RTX Pro 6000 GPU では、ファームウェア更新が失敗し、古いファームウェアバージョンのままになる場合があります。この問題は、特定のスペアユニットに限定され、更新プロセス全体には影響しません。	6.0(2.260044)	6.0(2.260069)

リリースで解決済みの問題 6.0(2.260044)

リリース 6.0(2.260044) では、次の問題が解決されました。

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済みリリース
CSCwb67315	プロファイルのデプロイメントワークフローが、LAN接続ポリシーとアダプタポリシーの検証手順中に次のエラーで失敗する場合があります。 エラーメッセージ： LAN接続ポリシーの検証 内部サーバーエラー：サーバー アダプタ スロットを取得できませんでした この問題は、リリースバージョン 4.3 以降のファームウェア バージョンを実行しているCisco UCS VICまたはMLOM アダプタを搭載した Intersight 管理対象スタンドアロンCisco UCS M7 またはM8 サーバーに影響を及ぼします。	6.0(1.250192)	6.0(2.260044)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済みリリース
CSCws30219	Cisco UCS M7 サーバは、ランタイム時にECCエラーが原因でホストロックが発生する場合があります。BIOSが変数を正しく取得できないため、EFI が無効なパラメータを返し、ログや Cisco IMC アラートなしでホストがフリーズします。ホストは応答不能になり、KVM 入力は受け入れられません。 この問題は解決されました。	4.3(6.250053)	6.0(2.260044)
CSCwb62117	Brocade SANスイッチと Dellstorage アレイに接続された LPe35002-M2 Emulex アダプタを搭載した Cisco UCS C240-M8 サーバで、断続的な I_T NexusLoss エラーが発生し、接続が不安定になり、LUNが定期的に切断されます。FCP I/O はエラーなしで完了しますが、アダプタは繰り返し接続の再確立を試みます。LOGO および FLOGI コマンドを発行することで、問題が再発する前に一時的に接続を復元します。 この問題は解決されました。	4.3(6.250053)	6.0(2.260044)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済みリリース
CSCwd55604	すべての Cisco UCS C245 M8 統合サーバの DIMM_P2_H1 は動作不能として報告されますが、すべての DIMM はメモリエラーなしで正常に機能します。この問題は、サーバがサポートされている同一の DIMM モデルを完全に装着しているにもかかわらず、機器の動作不能と互換性のないサーバファームウェアを示すアラートをトリガーします。 この問題は解決されました。	4.3(5.250001)	6.0(2.260044)
CSCwr82017	システムメモリ設定で Intel SGX Processor Reserved Memory Range Registers（PRMRR）のサイズがサポートされていないサイズに設定されている場合、Cisco UCS C220 M8 サーバおよび C240 M8 サーバは引き続きリセットされます。 この問題は解決されました。	6.0(1.250192)	6.0(2.260044)

不具合 ID	症状	影響を受ける最初のリリース	リリースで解決済み
CSCvr45526	特定の Cisco UCS サーバで、セキュアブートデータベース内の検証エラーが原因でブートの中断が発生します。この問題は、システムのスタートアップ中に特定のサーバモデルに影響を及ぼし、起動の中断を引き起こし、システムの信頼性に影響を与える可能性があります。この問題は、正常なセキュアブートプロセスを妨げるセキュア ブート データベース内の古い証明書が原因で発生します。 この問題は解決されました。	4.3(6.260017)	6.0(2.260044)

未解決の不具合

リリースで未解決の問題 6.0(2.260044)

リリース 6.0(2.260044) では、次の問題が未解決です。

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCwb41941	Cisco UCS C220 および C240 M8 サーバでは、Intel Secondary Service Processor（SSP）2.0 を使用するファームウェア バージョンは SSP 1.6 を使用する以前のリリースとの下位互換性がありません。 SSP 2.0 をサポートするファームウェアバージョンは次のとおりです。 4.3(6.260003)、6.0(1.250192)、6.0(2.260044) 以降 以前のバージョンにダウングレードすると、ベースボード管理コントローラ(BMC)がBIOS構成証明に失敗し、重要なシステムが不安定になります。 症状には、KVM コンソールでシステムがスタックする、起動の失敗、 POST のハング、致命的なエラー（CATERR）イベント、動作不能の NVMe デバイス、重大な温度しきい値のエラーを伴う温度センサーの障害などがあります。	以前のファームウェアバージョンにダウングレード、 BMC に障害が発生した場合は、次の回復手順を使用します。 1. BMC ファームウェアのアップグレード：:ホストソフトウェアアップグレード(HSU)または Cisco IMC インターフェイスを使用して、BMCファームウェアコンポーネントのみを最新バージョン（SSP 2.0 互換）にアップグレードします。 2. ホスト電源リセットの実行:ホストの電源を完全にリセットすると、システム状態の回復に役立つ場合がありますが、すべてのシナリオで 100% の効果があるとは限りません。	• 4.3(6.260003) • 6.0(1.250192) • 6.0(2.260044)

既知の動作と制限事項

リリース での既知の動作と制限事項 6.0(2.260044)

リリース 6.0(2.260044) では、既知の制限事項として次の問題があります。

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCwb34870	企業 OID（.1.3.6.1.4.1.9.9.719）に対して snmpget コマンドを実行すると、エラーが発生する場合があります。 さらに、それらの特定の OID で snmpget コマンドが失敗した場合、後続の snmpwalk 操作も失敗する可能性があります。 この問題は、リリースバージョン 6.0(2.260044)にアップグレードした後に発生します。	企業 OID（.1.3.6.1.4.1.9.9.719）で snmpget コマンドを実行しないようにしてください。 snmpget コマンドがすでに実行されていて、後続の snmpwalk 操作が失敗している場合、次のいずれかのアクションを実行して SNMP 機能を復元できます。 • Cisco IMC の再起動を実行します。 • SNMP サービスを無効にして、再度有効にします。	6.0(2.260044)

不具合 ID	症状	回避策	最初に影響を受けるリリース

CSCwr72707	Red Hat Enterprise Linux（(RHEL）OSを搭載した Cisco UCS C220 M8 システムで複数のドライブ（2 台以上）を同時に装着してテストすると、NVMe ドライブのランダムワークロードのパフォーマンスが大幅に低下します。具体的には、4K ランダム読み取りパフォーマンスは、同時動作中に、定格ドライブあたり 1,600k IOPS からドライブあたり約 680k IOPS に低下する可能性があります。	このパフォーマンスのボトルネックを解決するには、RHEL ブート設定で Intel が推奨する次のカーネル調整パラメータを適用します。
		• シングル ドライブ構成の場合: RHEL カーネル コマンド ラインに次を追加します。
		`intel_pstate=disable pcie_aspm.policy=performance pci=pcie_bus_safe`
		• マルチドライブ（完全装着）構成の場合：RHEL カーネル コマンド ラインに次を追加します。
		`intel_pstate=disable pcie_aspm.policy=performance pci=pcie_bus_safe nvme.poll_queues=32 intel_iommu=on`
			6.0(2.260044)

サポートされるプラットフォームとリリースの互換性マトリクス

このリリースでサポートされているプラットフォーム

このリリースでは、次のサーバがサポートされています。

- Cisco UCS C220 M8
- Cisco UCS C240 M8
- Cisco UCS C225 M8
- Cisco UCS C245 M8

- Cisco UCS C220 M7
- Cisco UCS C240 M7
- Cisco UCS C220 M6
- Cisco UCS C240 M6
- Cisco UCS C225 M6
- Cisco UCS C245 M6

これらのサーバの情報については、「サーバの概要」を参照してください。

Cisco IMC および Cisco UCS Manager リリース互換性マトリクス

Cisco Intersight、Cisco IMC、および Cisco UCS Manager 間のファームウェア バージョンの同等性

詳細については、「Cisco Intersight、Cisco IMC、および Cisco UCS Manager 向け Cisco UCS 同等性マトリクス」を参照してください。

Cisco IMC および Cisco UCS Manager リリース互換性マトリクス

Cisco UCS C シリーズ ラックマウント サーバは、内蔵スタンドアロン ソフトウェア (Cisco IMC) によって管理されます。しかし、ラックマウント サーバーを Cisco UCS Manager と統合すると、UCSM エンドユーザー インターフェイスを使用して、サーバーを管理します。

次の表には、ラックマウント サーバーのサポートされたプラットフォーム、Cisco IMC リリース、および Cisco UCS Manager リリースを示します。

表 *1 : Cisco IMC 6.0(2)* リリースのラックマウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
6.0(2.2600xx)	未定	• Cisco UCS C220 M8、C240 M8、C225 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
6.0(2.260069)	6.0(2c)	• Cisco UCS C220 M8、C240 M8、C225 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー
6.0(2.260044)	6.0(2b)	• Cisco UCS C220 M8、C240 M8、C225 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー

表 *2 : Cisco IMC 6.0(1)* リリースのラックマウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
6.0(1.250194)	NA	• Cisco UCS C240 M8 サーバ
6.0(1.250192)	6.0(1e)	• Cisco UCS C220 M8、C240 M8、C225 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
6.0(1.250174)	6.0(1d)	• Cisco UCS C220 M8、C240 M8、C225 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー
6.0(1.250131)	6.0(1c)	• Cisco UCS C220 M8、C240 M8、C225 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー
6.0(1.250130)	6.0(1b)	• Cisco UCS C245 M8 サーバー
6.0(1.250127)		• Cisco UCS C220 M8、C225 M8 および C240 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー

表 *3 : Cisco IMC 4.3(6)* リリースのラック マウント サーバー用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.3(6.2600xx)	未定	• Cisco UCS C220 M8、C225 M8、C240 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー • Cisco UCS S3260 M5 サーバ
4.3(6.260033)	未定	• Cisco UCS C220 M8、C225 M8、C240 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー • Cisco UCS S3260 M5 サーバ
4.3(6.260017)	4.3(6f)	• Cisco UCS C220 M8、C225 M8、C240 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー • Cisco UCS S3260 M5 サーバ

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.3(6.260003)	4.3(6e)	• Cisco UCS C220 M8 および C240 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー
4.3(6.250117)	N/A	• Cisco UCS C220 M7 サーバ
4.3(6.250101)	4.3(6d)	• Cisco UCS C220 M8、C225 M8、C240 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー • Cisco UCS S3260 M5 サーバ
4.3(6.250060)	N/A	• Cisco UCS C245 M8 サーバー
4.3(6.250053)	4.3(6c)	• Cisco UCS C220 M8、C225 M8、C240 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー • Cisco UCS S3260 M5 サーバ
4.3(6.250044)	4.3(6b)	• Cisco UCS C220 M8、C225 M8、C240 M8 および C245 M8 サーバー • Cisco UCS C220 M7 および C240 M7 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.3(6.250039)	4.3 (6a)	• Cisco UCS C220 M8 および C240 M8 サーバー • Cisco UCS S3260 M5 サーバ
4.3(6.250040)		• Cisco UCS C225 M8 および C245 M8 サーバ • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー

表 *4 : Cisco IMC 4.3(5)* リリースのラック マウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.3(5.250045)	NA	• Cisco UCS C225 M8 サーバー
4.3(5.250043)	NA	• Cisco UCS C225 M8 および C245 M8 サーバ
4.3(5.250033)	NA	• Cisco UCS C225 M8 および C245 M8 サーバ • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバーおよび S3260 M5 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.3(5.250030)	4.3(5d)	• Cisco UCS C225 M8 および C245 M8 サーバ • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバーおよび S3260 M5 サーバー
4.3(5.250001)	4.3(5c)	• Cisco UCS C225 M8 および C245 M8 サーバ • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバーおよび S3260 M5 サーバー
4.3(5.240021)	4.3(5a)	• Cisco UCS C225 M8 および C245 M8 サーバ • Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバーおよび S3260 M5 サーバー

表 *5 : Cisco IMC 4.3(4)* リリースのラック マウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
• 4.3(4.252002) • 4.3(4.252001)	NA	• 4.3(4.252002)：Cisco UCS C225 M6サーバー • 4.3(4.252001)：Cisco UCS C220 M6、C240 M6 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.3(4.242066)	4.3(4f)	• Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバーおよび S3260 M5 サーバー
4.3(4.242038)	NA	• Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバーおよび S3260 M5 サーバー
4.3(4.242028)	NA	• Cisco UCS C220 M7 および C240 M7 サーバー
4.3(4.241063)	4.3(4b)	• Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバーおよび S3260 M5 サーバー
4.3(4.241014)	4.3(4b)	Cisco UCS C245 M8 サーバ
4.3(4.240152)	4.3(4a)	• Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバーおよび S3260 M5 サーバー

表 *6 : Cisco IMC 4.3(3)* リリースのラック マウント サーバー用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.3(3.240043)	NA	• Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー
4.3(3.240041)	NA	• Cisco UCS S3260 M5 サーバ
4.3(3.240022)	4.3 (3a)	• Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6 および C245 M6 サーバーおよび S3260 M5 サーバー

表 *7 : Cisco IMC 4.3(2)* リリースのラック マウント サーバー用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.3(2.260007)	4.3(6f)	Cisco UCS C220 M5、C240 M5、C480 M5 および C125 M5 サーバ。
4.3(2.250063)	NA	Cisco UCS C220 M5、C240 M5、C480 M5 および C125 M5 サーバ。
4.3(2.250045)	NA	Cisco UCS C220 M5、C240 M5、C480 M5 および C125 M5 サーバ。
4.3(2.250037)	4.3(6c)	Cisco UCS C220 M5、C240 M5、C480 M5 サーバー
4.3(2.250022)	N/A	Cisco UCS C125 M5 サーバー
4.3(2.250021)	NA	Cisco UCS C240 M5 サーバー
4.3(2.250016)	NA	Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.3(2.240107)	NA	Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー
4.3(2.240090)	NA	Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー
4.3(2.240077)	NA	Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー
4.3(2.240053)	NA	Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー
4.3(2.240037)	NA	• Cisco UCS C225 M6、および C245 M6 サーバー
4.3(2.240009)	NA	• Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー • Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー
4.3(2.240002)	4.3(2)	• Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー • Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.3(2.230270)	4.3(2)	• Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー • Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー
4.3(2.230207)	4.3(2)	• Cisco UCS C220 M7 および C240 M7 サーバー • Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 サーバー • Cisco UCS C220 M5、C240 M5、C480 M5、C125 M5 および S3260 M5 サーバー

表 *8 : Cisco IMC 4.3(1)* リリースのラック マウント サーバー用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.3(1.230138)	サポートなし	Cisco UCS C220 M7 および C240 M7 サーバー
4.3(1.230124)	サポートなし	Cisco UCS C220 M7 および C240 M7 サーバー
4.3(1.230097)	サポートなし	Cisco UCS C220 M7 および C240 M7 サーバー

表 *9 : Cisco IMC 4.2(3)* リリースのラック マウント サーバー用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.2(3q)	NA	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5、および C125 M5 サーバ

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.2(3p)	4.2 (3o)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M5、および C125 M5 サーバ
4.2(3o)	4.2(3n)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.2(3n)	4.2(3m)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.2(3m)	4.2(3l)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.2(3l)	4.2(3k)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.2(3k)	NA	Cisco UCS S3260 M5 サーバ
4.2(3j)	4.2(3j)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.2(3i)	4.2(3i)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.2(3g)	4.2(3g)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.2(3e)	4.2(3e)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.2(3d)	4.2(3d)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.2(3b)	4.2(3b)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー

表 *10 : Cisco IMC 4.2(2)* リリースのラック マウント サーバー用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.2（2g）	4.2(2d)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.2(2f)	4.2(2c)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.2(2a)	4.2 (2a)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー Cisco UCS C220 M5、C240 M5、C240 SD M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー

表 *11 : Cisco IMC 4.2(1)* リリースのラック マウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.2(1j)	4.2(1n)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1i)	4.2(1m)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1g)	サポートなし	Cisco UCS C225 M6、および C245 M6 サーバー
4.2(1f)	4.2(1k)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1e)	4.2(1i)	Cisco UCS C220 M6、C225 M6、C240 M6、および C245 M6 サーバー
4.2(1c)	サポートなし	Cisco UCS C225 M6、および C245 M6 サーバー
4.2(1b)	4.2(1f)	Cisco UCS C220 M6、および C240 M6 サーバー
4.2(1a)	4.2(1d)	Cisco UCS C220 M6、C240 M6、および C245 M6 サーバー （注） Cisco UCS Manager は、Cisco UCS C245 M6 サーバーをサポートしません。

表 *12 : Cisco IMC 4.1(3)* リリースのラック マウント サーバー用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.1(3n)	NA	Cisco UCS C220 M5、C240 M5、C480 M5 および S3260 M5 および S3260 M4 サーバー
4.1(3m)	4.1(3m)	Cisco UCS C220 M5、C240 M5、C480 M5 および S3260 M5 および S3260 M4 サーバー
4.1(3l)	4.1(3k)	Cisco UCS C480 M5、C220 M5、および C240 M5 サーバー
4.1(3i)	4.1(3j)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M4、S3260 M5、C125 M5 サーバー
4.1(3h)	4.1(3i)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M4、S3260 M5、C125 M5 サーバー
4.1(3g)	サポートなし	Cisco UCS S3260 M4 および S3260 M5 サーバ
4.1(3f)	4.1(3h)	Cisco UCS C220 M5、C240 M5、C480 M5、S3260 M4、S3260 M4、S3260 M5、および C125 M5 サーバー
4.1（3d）	4.1(3e)	Cisco UCS C220 M5、C240 SD M5 、C240 M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.1（3c）	4.1（3d）	Cisco UCS C220 M5、C240 SD M5 、C240 M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー
4.1（3b）	4.1(3a)	Cisco UCS C220 M5、C240 SD M5 、C240 M5、C480 M5、C480 ML M5、S3260 M4、S3260 M5、および C125 M5 サーバー

表 *13 : Cisco IMC 4.1(2)* リリースのラック マウント サーバー用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.1(2m)	サポートなし	Cisco UCS C220 M4、C240 M4、および C460 M4 サーバー。
4.1(2l)	サポートなし	Cisco UCS C220 M4、C240 M4 サーバー。
4.1(2k)	サポートなし	Cisco UCS C220 M4、C240 M4、および C460 M4 サーバー
4.1(2j)	サポートなし	Cisco UCS C220 M4、C240 M4、および C460 M4 サーバー
4.1(2h)	サポートなし	Cisco UCS C220 M4、C240 M4、および C460 M4 サーバー
4.1(2g)	サポートなし	Cisco UCS C220 M4、C240 M4、および C460 M4 サーバー
4.1(2f)	4.1（2c）	Cisco UCS C220 M5、C240 SD M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバー
4.1(2e)	サポートなし	Cisco UCS C125 M5 サーバー
4.1(2d)	サポートなし	Cisco UCS C240 M5 および C240 SD M5 サーバー
4.1(2b)	4.1(2b)	Cisco UCS C220 M5、C240 SD M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバー
4.1(2a)	4.1(2a)	Cisco UCS C220 M5、C240 SD M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバー

表 *14 : Cisco IMC 4.1(1)* リリースのラック マウント サーバ用 *Cisco IMC* および *UCS Manager* ソフトウェア リリース

Cisco IMC のリリース	Cisco UCS Manager リリース	ラックマウント サーバ
4.1(1h)	4.1(1e)	Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.1(1g)	4.1(1d)	Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.1(1f)	4.1(1c)	Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ
4.1(1d)	4.1(1b)	Cisco UCS C220 M5、C240 M5、C480 M5、および C480 ML M5 サーバ
4.1(1c)	4.1(1a)	Cisco UCS C220 M5、C240 M5、C480 M5、C480 ML M5、S3260 M5、C125 M5、C220 M4、C240 M4、C460 M4、および S3260 M4 サーバ

ファームウェア ファイル

ファームウェア ファイル

C シリーズのソフトウェア リリース バージョン6.0(2.260044) には、次のソフトウェア ファイルが含まれます。

CCO ソフトウェア タイプ	ファイル名	備考
Unified Computing System（UCS）サーバ ファームウェア	リリース特有の ISO バージョンについては、Cisco UCS C シリーズ統合管理コントローラ ファームウェア ファイル、リリース 6.0 を参照してください。	ホスト アップグレード ユーティリティ

Unified Computing System（UCS）ドライバ	ucs-cxxx-drivers6.0(2.260044).iso ucs-cxxx-drivers6.0(2.260044).iso	ドライバ
Unified Computing System（UCS）ユーティリティ	ucs-cxxx-utils-efi6.0(2.260044).iso ucs-cxxx-utils-linux6.0(2.260044).iso ucs-cxxx-utils-vmware6.0(2.260044).iso ucs-cxxx-utils-windows6.0(2.260044).iso	ユーティリティ

（注） 必ず BIOS、Cisco IMC および CMC を HUU ISO からアップグレードしてください。予期しない動作の原因となる場合があるため、コンポーネント（BIOS のみ、または Cisco IMC のみ）を個別にアップグレードしないでください。BIOS をアップグレードし、HUU ISO からではなく、Cisco IMC を個別にアップグレードすることを選択した場合は、Cisco IMC と BIOS の両方を同じコンテナリリースにアップグレードしてください。

BIOS と Cisco IMC のバージョンが異なるコンテナリリースからのものである場合、予期しない動作が発生する可能性があります。Cisco IMC、BIOS、およびその他すべてのサーバコンポーネント (VIC、RAID コントローラ、PCI デバイス、および LOM) のファームウェアバージョンを更新するには、Host Upgrade Utility から [すべて更新 (Update All)] オプションを使用することを推奨します。

ホスト アップグレード ユーティリティ

Cisco Host Upgrade Utility (HUU) は、Cisco UCS C シリーズファームウェアをアップグレードするツールです。

ファームウェアのイメージファイルは、ISO に埋め込まれています。ユーティリティにメニューが表示され、これを使用してアップグレードするファームウェア コンポーネントを選択することができます。このユーティリティに関する詳細については、http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html を参照してください。

個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、Cisco UCS C シリーズ統合管理コントローラファームウェアファイル、リリース 6.0 を参照してください。

ファームウェアの更新

Host Upgrade Utility を使用して、C シリーズのファームウェアを更新します。Host Upgrade Utility は、次のソフトウェア コンポーネントをアップグレードできます。

- BIOS
- Cisco IMC
- CMC
- Cisco VIC アダプタ

- Broadcom アダプタ
- オンボード LAN
- PCIe アダプタ ファームウェア
- HDD ファームウェア
- SAS エクスパンダ ファームウェア
- DCPMM メモリ
- PCI Gen5 リタイマー

すべてのファームウェアは、サーバが正常に動作するようにまとめてアップグレードする必要があります。

（注） Cisco IMC、BIOS、およびその他のすべてのサーバー コンポーネント（VIC、RAID コントローラ、PCI デバイス、および LOM）のファームウェア バージョンを更新するには、ホスト更新ユーティリティからすべての選択して、**[更新]** または **[更新とすべての更新して有効化（Update & Activate All）]** オプションを使用することをお勧めします。ファームウェアを導入したら、**[終了 (Exit)]** をクリックします。

ユーティリティを使用してファームウェアをアップグレードする方法の詳細については、次を参照してください。

http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-user-guide-list.html

サポート対象ハードウェアおよびソフトウェア

オペレーティング システムとブラウザの要件

サポートされているオペレーティング システムの詳細については、インタラクティブな『UCS ハードウェアおよびソフトウェアの互換性』マトリックスを参照してください。

Cisco では、Cisco UCS ラック サーバ ソフトウェア、リリース 6.0(2) に次のブラウザを推奨しています。

推奨されるブラウザ	推奨されるブラウザの最小バージョン	推奨される最小オペレーティング システム
Google Chrome	バージョン 143.0.7499.193（公式ビルド）（arm64）	Mac OS 26.2
	バージョン 143.0.7499.193	Microsoft Windows 11 (10.0.26200)
	バージョン 143.0.7499.193	Microsoft Windows 11 (26200.7462)
	Microsoft Edge バージョン 143.0.3650.139（公式ビルド）（64 ビット）	
Safari	バージョン 26.2（21623.1.14.11.9）	Mac OS 26.2
	バージョン 26.2（21623.1.14.11.9）	
Mozilla Firefox	バージョン 146.0.1 (aarch64)	
	バージョン 146.0.1	Microsoft Windows 11 (10.0.26200)
Microsoft Edge	バージョン 143.0.3650.139	

（注） 管理クライアントがサポートされていないブラウザを使用して開始されている場合、サポートされているブラウザ バージョンのログイン ウィンドウで入手可能な「サポートされたブラウザの最も良い結果のために」のオプションからのヘルプ情報を確認してください。

Transport Layer Security（TLS）バージョン 1.3

デフォルトポート

次に示すのは、サーバ ポートとそのデフォルトのポート番号のリストです。

表 *15*：サーバ ポート

ポート名	ポート番号
LDAP Port 1	389
LDAP Port 2	389
LDAP Port 3	389
LDAP Port 4	3268

ポート名	ポート番号
LDAP Port 5	3268
LDAP Port 6	3268
SSHポート	22
[HTTP ポート（HTTP Port）]	80
HTTPS ポート	443
SMTP ポート（SMTP Port）	25
KVM ポート	2068
Intersight 管理ポート	8889
Intersight クラウド ポート	8888
SOL SSH ポート	2400
SNMPポート	161
SNMP トラップ	162
外部Syslog	514

リリース 6.0(2) へのアップグレード パス

Cisco IMC で可能なすべてのアップグレードパスの完全な概要を取得するには、Cisco UCS ラック サーバー アップグレード サポート マトリックスを参照してください。

SNMP

このリリース以降のリリースでサポートされている MIB 定義については、次のリンクを参照してください。

https://cisco.github.io/cisco-mibs/

ソフトウェア ユーティリティ

次の標準ユーティリティを使用できます。

- Host Update Utility（HUU）
- BIOS および Cisco IMC ファームウェアのアップデート ユーティリティ
- サーバ設定ユーティリティ (SCU)
- サーバ診断ユーティリティ (SDU)

ユーティリティ機能は次のとおりです。

- USB 上の HUU、SCU のブート可能なイメージとしての可用性。USB にはドライバ ISO も含まれており、ホストのオペレーティングシステムからアクセスできます。

関連資料

このリリースの設定については、次を参照してください。

- 『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide』
- 『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』
- Cisco UCS ラックマウント サーバ Cisco IMC API プログラマ ガイド

C シリーズサーバのインストールの詳細については、次を参照してください。

- Cisco UCS C シリーズラックサーバのインストールおよびアップグレードガイド

次の関連資料は、Cisco Unified Computing System（UCS）で入手できます。

- 『Regulatory Compliance and Safety Information for Cisco UCS』
- 管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、「Release Bundle Contents for Cisco UCS Software」を参照してください。

次の場所にある『Cisco UCS Manager ソフトウェアのリリースノート』および『 *Cisco UCS C* シリーズの *Cisco UCS Manager* との統合に関するガイド』を参照してください。

- 『Cisco UCS Manager Release Notes』
- Cisco UCS C シリーズ サーバと Cisco UCS Manager との統合に関するガイド

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。