



「Cisco Intersight サーバファームウェアのリリースノート、リリース 6.0」を参照してください

最終更新：2026 年 10 月 2 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025–2026 Cisco Systems, Inc. All rights reserved.



第 1 章

Cisco Intersight 管理モード サーバファームウェア、リリース 6.0

- [Cisco Intersight 管理モード サーバファームウェア、リリース 6.0](#) (1 ページ)
- [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](#) (2 ページ)
- [サポート終了の Intersight 管理モード サーバでサポートされる最後のファームウェア](#) (3 ページ)
- [更新履歴](#) (3 ページ)

Cisco Intersight 管理モード サーバファームウェア、リリース 6.0

Cisco Intersight 管理モードのサーバーファームウェアアップデートは、Intersight を介して管理される、サポート対象の Cisco UCS サーバーおよび Cisco Unified Edge サーバー向けに、BIOS、CIMC、アダプター、その他のサーバーコンポーネントの更新版を提供するものです。サーバーファームウェア、Cisco UCS サーバーファームウェアを管理するには、[Intersight 管理モードでのファームウェアの管理](#) およびユニファイド Edge コンピューティング ノードのファームウェアのアップグレードを参照してください。この機能は、Cisco Intersight Essentials または Advanced ライセンス階層で使用できます。



(注) このドキュメントでは、これらの IMM サーバに関連する既知の問題と制限事項についてのみ説明します。

Intersight で管理されるサポート対象のサーバーは次のとおりです：

- **Intersight 管理モード (IMM) サーバ**

次のようなものがあります。

- Edge Chassis Management Controller (eCMC) を介して Intersight に接続された Cisco UCS XE シリーズ ユニファイド Edge サーバー。
- Cisco UCS Fabric Interconnect (FI) を介して Intersight に接続された Cisco UCS X シリーズ、B シリーズ、および C シリーズ サーバー。

• **Intersight スタンドアロン モード サーバ :**

これには、ファブリック インターコネクト アタッチメントのない Cisco UCS C シリーズ および S シリーズ ラック サーバが含まれます。Cisco 統合管理コントローラ (CIMC) によって管理されます。ISM サーバに関連する既知の問題と制限については、[Cisco IMC リリース ノート](#)を参照してください。

• **UCS Manager (UCSM) 管理モード (UMM) サーバ :**

これには、ファブリック インターコネクト (FI) に接続され、UCS Manager で管理される Cisco UCS B シリーズ、C シリーズ、X シリーズ、S シリーズ、および HX シリーズ サーバが含まれます。

UMM サーバに関連する既知の問題と制限については、[Cisco UCS Manager リリース ノート](#)を参照してください。

• **Cisco UCS C885A M8 ラック サーバ :**

Cisco UCS C885A M8 ラック サーバに関連する既知の問題と制限については、[Cisco UCS C885A M8 ラック サーバの Cisco ベースボード管理コントローラ リリース ノート](#)を参照してください。

• **Cisco UCS C845A M8 ラック サーバ :**

Cisco UCS C845A M8 ラック サーバに関連する既知の問題と制限については、[Cisco ベースボード管理コントローラ 2.0 リリース ノート](#)、[リリース 2.0](#)を参照してください。

Intersight のファームウェアアップグレードには、サーバとインフラストラクチャファームウェアの更新の両方が含まれており、個別に更新できます。つまり、最新のサーバファームウェアを使用するために Fabric Interconnect や Unified Edge Chassis Management Controller (eCMC) のインフラストラクチャファームウェアを必ずしもアップグレードする必要はなく、その逆も同様です。インフラストラクチャファームウェアとサーバファームウェア間の互換性の詳細については、[クロスバージョンのファームウェア サポート](#)を参照してください。インフラストラクチャファームウェアのアップデートに関する詳細については、「[Cisco Intersight Managed Mode Infrastructure Firmware のリリース ノート](#)」および「[Cisco Intersight Unified Edge eCMC Infrastructure Firmware のリリース ノート](#)」を参照してください。

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。

完全なマトリックスをPDF形式で表示するには、[ここ](#)をクリックしてください。

サポート終了の Intersight 管理モード サーバでサポートされる最後のファームウェア

プラットフォーム	サポートされる最後のファームウェアバージョン
Cisco UCS C シリーズ M5 (C220、C240、C480)	4.3(2.260007)
Cisco UCS C シリーズ M6 (C220、C240)	4.3 (6.260054)
Cisco UCS B シリーズM5 (B200、B480)	5.4 (0.260050)
Cisco UCS B シリーズM6 (B200)	5.4 (0.260050)

詳細については、[C シリーズ サーバーのサポート終了および販売終了のお知らせ](#) および [B シリーズサーバーのサポート終了および販売終了のお知らせ](#)を参照してください。

更新履歴

次の表は、このマニュアルの改訂履歴を含んだものです。

表 1: リリース 6.0.2

改訂日	説明
2026 年 4 月 23 日	次のサーバーファームウェアリリースバージョンのリリースノートを更新しました。 • Cisco UCS X シリーズ M8、M7、および M6 サーバーファームウェアリリース 6.0(2.260069) • Cisco UCS C シリーズ M8、M7 および M6 サーバーファームウェアリリース 6.0(2.260069) • Cisco UCS B シリーズ M6 サーバーファームウェアリリース 6.0(2.260069) このリリースには、以下への更新が含まれます。 • 新しいハードウェア • セキュリティ修正 • 解決済みの問題 • 未解決の問題

改訂日	説明
2026 年 3 月 16 日	次のサーバー ファームウェア リリース バージョンのリリース ノートを更新しました。 • Cisco UCS X シリーズ M8、M7、および M6 サーバー ファームウェア リリース 6.0(2.260040) • Cisco UCS XE シリーズ M8 サーバー ファームウェア リリース 6.0(2.260042) • Cisco UCS C シリーズ M8、M7 および M6 サーバー ファームウェア リリース 6.0(2.260044) • Cisco UCS B シリーズ M6 サーバー ファームウェア リリース 6.0(2.260040) このリリースには、以下への更新が含まれます。 • 新しいハードウェア • セキュリティ修正 • 解決済みの問題 • 未解決の問題 • 既知の問題

表 2: リリース 6.0.1

改訂日	説明
2026 年 3 月 27 日	Intersight インフラストラクチャ ファームウェア バージョン 6.0(1.260006) がリリースされました。対応するサーバファームウェア リリースはありません。

改訂日	説明
2026 年 3 月 16 日	次のサーバファームウェアリリースバージョンのリリース ノートを更新しました。 • Cisco UCS B シリーズ M5 サーバー ファームウェア リリース 6.0(1.260012) このリリースには、以下への更新が含まれます。 • 解決済みの問題 • セキュリティ修正 新しいハードウェアや未解決の問題は含まれていません。
2026 年 2 月 6 日	Intersight インフラストラクチャ ファームウェア バージョン 6.0(1.260003) がリリースされました。対応するサーバファームウェアリリースはありません。
2026 年 1 月 16 日	次のサーバファームウェアリリースバージョンのリリース ノートを更新しました。 • Cisco UCS XE シリーズ M8 サーバー ファームウェア リリース 6.0(1.260001) このリリースには、以下への更新が含まれます。 • XE シリーズ M8 サーバファームウェア リリース 6.0(1.260001) の解決済みの問題 (58 ページ) 新しいハードウェア、セキュリティ修正、未解決の問題は含まれていません。

改訂日	説明
2026 年 1 月 14 日	Cisco UCS C シリーズ M8 サーバファームウェア、リリース 6.0(1.250194) のリリース ノートを更新しました。 このリリースには、Cisco UCS C220 M8 に影響するクリティカルな電源投入の問題に対処する BMC ファームウェアの更新が含まれています。 新しいハードウェア、セキュリティ修正、解決済みの問題、未解決の問題は含まれていません。

改訂日	説明
2025 年 12 月 18 日	次のサーバー ファームウェア リリース バージョンのリリース ノートを更新しました。 • Cisco UCS X シリーズ M7 および M6 サーバー ファームウェア、リリース 6.0(1.250179) • Cisco UCS X シリーズ M8 サーバー ファームウェア リリース 6.0(1.252114) • Cisco UCS B シリーズ M6 および M5 サーバー ファームウェア リリース 6.0(1.250169) • Cisco UCS C シリーズ M8、M7 および M6 サーバー ファームウェア リリース 6.0(1.250192) このリリースには、以下への更新が含まれます。 • Cisco UCS X シリーズ M7 6.0(1.250179) および C シリーズ M7、M6 6.0(1.250192) サーバファームウェア リリースの解決済みの問題 (60 ページ) • X シリーズ M8 6.0(1.252114) および C シリーズ M8 6.0(1.250192) サーバファームウェア リリースの未解決の問題 (72 ページ) 新しいハードウェアのサポートや未解決の問題は含まれていません。 Cisco UCS X580p PCIe ノードのファームウェアバージョン 6.0(1.252050) および Cisco UCS X9508 シャーシのファームウェアバージョン 6.0(1.252050) がリリースされました。
2025 年 12 月 12 日	以下の各セクションが更新されました。 • Cisco UCS X シリーズ M8 サーバファームウェア リリース 6.0(1.252039) の新しいハードウェア (21 ページ) には、Cisco UCS X580p PCIe ノードと Cisco UCS X9516 X-Fabric のサポートが含まれています。

改訂日	説明
2025 年 12 月 1 日	次のサーバファームウェアリリースバージョンのリリース ノートを更新しました。 • Cisco UCS XE シリーズ M8 サーバファームウェア リリース 6.0(1.251030) このリリースには、以下への更新が含まれます。 • Cisco UCS XE シリーズ M8 サーバファームウェア リリース 6.0(1.251030) の新しいハードウェア (18 ページ) • XE シリーズ M8 サーバファームウェア リリース 6.0(1.251030) の未解決の問題 (73 ページ) • XE シリーズ M8 サーバファームウェア リリース 6.0(1.251030) の既知の問題 (84 ページ) 解決済みの不具合は含まれていません。
2025 年 11 月 21 日	Cisco UCS X シリーズ M8 サーバファームウェア、リリース 6.0(1.252039) のリリース ノートを更新しました。 新しいハードウェア、セキュリティ修正、解決済みの問題、未解決の問題は含まれていません。

改訂日	説明
2025 年 11 月 12 日	次のサーバー ファームウェア リリース バージョンのリリース ノートを更新しました。 • Cisco UCS X シリーズ M8、M7、および M6 サーバー ファームウェア リリース 6.0(1.250162) • Cisco UCS B シリーズ M6 および M5 サーバー ファームウェア リリース 6.0(1.250157) • Cisco UCS C シリーズ M8、M7 および M6 サーバー ファームウェア リリース 6.0(1.250174) このリリースには、以下への更新が含まれます。 • C シリーズ M8、M7、M6 6.0(1.250174) サーバファームウェア リリースのセキュリティ修正 (48 ページ) • Cisco UCS X シリーズ M8 6.0(1.250162) および C シリーズ M8、M6 6.0(1.250174) サーバファームウェア リリースの解決済みの問題 (61 ページ) 新しいハードウェアや未解決の問題は含まれていません。

改訂日	説明
2025 年 10 月 9 日	次のサーバー ファームウェア リリース パージョンのリリース ノートを更新しました。 • Cisco UCS X シリーズ M8、M7、および M6 サーバ ファームウェア リリース 6.0(1.250122) • Cisco UCS B シリーズ M6 および M5 サーバ ファームウェア リリース 6.0(1.250127) • Cisco UCS C シリーズ M8、M7 および M6 サーバ ファームウェア リリース 6.0(1.250131) このリリースには、以下への更新が含まれます。 • Cisco UCS X シリーズ M8、M7 6.0(1.250122)、M6、B シリーズ M6、M5 6.0(1.250127) および C シリーズ M8、M7、M6 6.0(1.250131)サーバファームウェア リリースの解決済みの問題 (65 ページ) 新しいハードウェア、セキュリティ修正、未解決の問題は含まれていません。

改訂日	説明
2025 年 9 月 2 日	次のサーバファームウェアリリースバージョンのリリース ノートを作成しました。 • Cisco UCS X シリーズ M8、M7、および M6 サーバファームウェア リリース 6.0(1.250120) • Cisco UCS B シリーズ M6 および M5 サーバファームウェア リリース 6.0(1.250126) • Cisco UCS C シリーズ M8、M7 および M6 サーバファームウェア リリース 6.0(1.250127) • Cisco UCS C シリーズ M8 (6.0(1.250127)、6.0(1.250130))、M7 (6.0(1.250127))、および M6 (6.0(1.250127)) サーバファームウェア リリース このリリースには、以下への更新が含まれます。 • Cisco UCS X シリーズ M8、M7、M6 6.0(1.250120) および C シリーズ M8、M7、M6 6.0(1.250127) サーバファームウェア リリースの新しいハードウェア (23 ページ) • Cisco UCS X シリーズ M8、M7、M6 6.0(1.250120)、B シリーズ M6、M5 6.0(1.250126) および C シリーズ M8、M7、M6 6.0(1.250127) サーバファームウェア リリース (50 ページ) • Cisco UCS C シリーズ M8、M7 および M6 6.0(1.250127) サーバファームウェア リリースで解決された不具合 (66 ページ) • Cisco UCS X シリーズ M8、M7 6.0(1.250120)、M6、B シリーズ M6、M5 6.0(1.250126) および C シリーズ M8、M7、M6 6.0(1.250127) サーバファームウェア リリースの未解決の問題 (76 ページ) • Cisco UCS C シリーズ M8、M7 および M6 6.0(1.250127) サーバファームウェア リリースの既知の問題 (86 ページ)



第 2 章

新しいソフトウェア機能

- [新しいソフトウェア機能 \(13 ページ\)](#)

新しいソフトウェア機能

Intersight ソフトウェア機能では、Intersight ファームウェア リリース スケジュールに一致しない場合があります。最新のソフトウェア機能についての詳細は、Intersight ヘルプ センターの「[新機能](#)」セクションを参照してください。



第 3 章

新しいハードウェア機能

- Cisco UCS X シリーズ M8、M7 6.0(2.260069) および C シリーズ M8 6.0(2.260069) サーバーファームウェア リリースの新しいハードウェア (16 ページ)
- Cisco UCS B シリーズ M5 6.0(1.260012) サーバーファームウェア リリースの新しいハードウェア：なし (16 ページ)
- Cisco UCS X シリーズ M8、M7 サーバファームウェア リリース 6.0(2.260040) の新しいハードウェア (16 ページ)
- Cisco UCS XE シリーズ M8 サーバファームウェア リリース 6.0(1.260001) の新しいハードウェア：なし (18 ページ)
- Cisco UCS C シリーズ M8 サーバファームウェア リリース 6.0(1.250194) の新しいハードウェア：なし (18 ページ)
- Cisco UCS X シリーズ M8、M7 6.0(1.252114)、M6、B シリーズ M66.0(1.250179)、M56.0(1.250169) および C シリーズ M8、M7、M6 6.0(1.250192) サーバファームウェア リリースで新しいハードウェア：なし (18 ページ)
- Cisco UCS XE シリーズ M8 サーバファームウェア リリース 6.0(1.251030) の新しいハードウェア (18 ページ)
- Cisco UCS X シリーズ M8 サーバファームウェア リリース 6.0(1.252039) の新しいハードウェア (21 ページ)
- Cisco UCS X シリーズ M8、M7、M6 6.0(1.250162)、B シリーズ M6、M56.0(1.250157)、および C シリーズ M8、M7、M6 6.0(1.250174) サーバファームウェア リリースで新しいハードウェア：なし (22 ページ)
- Cisco UCS X シリーズ M8、M7 6.0(1.250122)、M6、B シリーズ M66.0(1.250127)、M56.0(1.250131) および C シリーズ M8、M7、M6 サーバファームウェア リリースの新しいハードウェア：なし (23 ページ)
- Cisco UCS X シリーズ M8、M7、M6 6.0(1.250120) および C シリーズ M8、M7、M6 6.0(1.250127) サーバーファームウェア リリースの新しいハードウェア (23 ページ)

Cisco UCS X シリーズ M8、M7 6.0(2.260069) および C シリーズ M8 6.0(2.260069) サーバー ファームウェア リリースの新しいハードウェア

- Cisco UCS C245 M8 および C240 M8 および C240 M7 サーバの NVIDIA OEM BlueField-3 B3220 DPU 2x200G QSFP112、暗号化無効 (UCSC-P-N3220)。
- Cisco UCS C225 M8、C245 M8、C220 M8、C240 M8 および C240 M7 サーバ上の UCS NVIDIA BlueField-3 B3220L SuperNIC 2x200G QSFP112、PCIe Gen5.0 x16、暗号無効 (UCSC-P-N3220L)
- Cisco UCS C245 および C240 M8 サーバーでの NVIDIA Crypto B3220 Data Processing Unit (DPU) (UCSC-P-NC3220) のサポート。
- Cisco UCS C240、C220、X215c、および X210c M8 サーバでの 30 TB E3.S TLC Micron 9550 ドライブのサポート
- Cisco UCS C240、C220、X215c、および X210c M8 サーバでの E3.S FIPS (Kioxia CM -7) ドライブのサポート

Cisco UCS B シリーズ M5 6.0(1.260012) サーバー ファームウェア リリースの新しいハードウェア：なし

Cisco UCS X シリーズ M8、M7 サーバ ファームウェア リリース 6.0(2.260040) の新しいハードウェア

- X シリーズ M8 6.0(2.260040) サーバ ファームウェア

Cisco UCS X410c M8 コンピューティング ノード

Cisco UCS X410c M8 コンピュータ ノードは、Cisco UCS X シリーズ モジュラー システム 向けに専用設計された、第 2 世代の 4 ソケット コンピュータ ノードです。

7 ラックユニット (7 RU) Cisco UCS X9508 サーバシャーシは、最大 4 台の Cisco UCS X410c M8 コンピューティング ノードをサポートします。この設定は、多様なワークロードに適応する柔軟性を提供します。

Cisco UCS X410c M8 コンピューティング ノードの主な機能は次のとおりです。

- CPU : Intel Xeon 6 プロセッサ 4 基 (各プロセッサ最大 86 コア)

- **メモリ** : 256GB DDR5-6400 DIMM を 64 枚使用し、最大 16 TB のメインメモリを搭載可能。
- **ストレージ** : ノードは次のストレージ構成をサポートします。
 - 最大 9 台のホットプラグ可能な EDSFF E3.S NVMe ドライブと、パススルー フロント メザニン コントローラ。
 - エンタープライズクラスの RAID オプションを備えた、ホットプラグ対応の 2.5 インチ Solid-State Drives (SSDs) または Non-Volatile Memory Express (NVMe) ドライブを最大 6 台搭載可能。
 - 最大 2 台の M.2 SATA または NVMe ドライブにより、ブートとローカルストレージを実現。
- **mLOM 仮想インターフェイスカード (VIC)** : ノードは、次のモジュール型 LAN on マザーボード (mLOM) オプションをサポートします。
 - Cisco UCS VIC 15420 : 各インテリジェント ファブリック モジュール (IFM) へのユニファイドファブリック接続の最大 50 Gbps (2x 25 Gbps) を可能にします。
 - Cisco UCS VIC 15230 : 各 IFM への最大 100 Gbps でのユニファイドファブリック接続を可能にします。
- **オプションのメザニンカード** : オプションの第 5 世代 Cisco UCS VIC 15422 は、メザニン スロットを占有します。ブリッジカードはネットワーク接続を拡張し、サーバあたり 200 Gbps の合計帯域幅を提供します。
- **セキュリティ** : オプションの TPM (Trusted Platform Module) 、セキュアブート対応 FPGA、および ACT2 偽造防止機能へのサポート。

詳細については、[Cisco UCS X410c M8 コンピューティング ノード データ シート](#) および [Cisco UCS X410c M8 コンピューティング ノード スペック シート](#) を参照してください。

• X シリーズ M7 6.0(2.260040) サーバファームウェア

Cisco UCS X210c M7 サーバでの Cisco UCS X580p PCIe ノードのサポート

Cisco UCS X210c M7 サーバでの Cisco UCS X580p PCIe ノードのサポートが追加されました。UCSX-GPU-H200-NVL および UCSX-GPU-RTXP6000 GPU は、X580p PCIe ノードで使用する場合、Cisco UCS X210c M7 サーバでサポートされます。



(注)

- UCSX-GPU-L40S GPU は、X580p PCIe ノードで使用する場合、現在 Cisco UCS X210c M7 サーバではサポートされていません。
- X580p PCIe ノードを搭載した Cisco UCS X210c M7 サーバのサポートは、第 5 世代インテル Xeon Scalable processor (Emerald Rapids) を使用している場合にのみ使用できます。

Cisco UCS XE シリーズ M8 サーバファームウェア リリース 6.0(1.260001) の新しいハードウェア：なし

Cisco UCS C シリーズ M8 サーバファームウェア リリース 6.0(1.250194) の新しいハードウェア：なし

Cisco UCS X シリーズ M8、M7 6.0(1.252114)、M6、B シリーズ M6 6.0(1.250179)、M5 6.0(1.250169) および C シリーズ M8、M7、M6 6.0(1.250192) サーバファームウェア リリースで新しいハードウェア：なし

Cisco UCS XE シリーズ M8 サーバファームウェア リリース 6.0(1.251030) の新しいハードウェア

Cisco UCS XE130c M8 コンピューティング ノード

Cisco Unified Edge は、コンピューティング、ストレージ、ルーティング、スイッチング、およびセキュリティを単一の構成可能なソリューションに統合し、IT 組織がグローバル規模でエッジインフラインフラストラクチャのデプロイメント、運用、ライフサイクル管理を簡素化できるようにします。

Cisco Unified Edge は、3RU の奥行き短いマルチマウント可能なシャーシを備えたモジュラエッジプラットフォームで、拡張された温度範囲（5 ～ 45 °C）で動作し、静音プロファイル（25 °で 40s dBA）を維持する機能を備えています。C および 20% PWM をサポートし、高微粒子環境に対する保護機能を提供し、物理に幅広いスペースへの展開を可能にします。

Cisco UCS XE130c M8 は、1RU、ハーフ幅のコンピューティング ノードファミリです。Cisco UCS XE9305 シャーシには、最大 5 つの Cisco UCS XE130c M8 コンピューティング ノードを収容できます。企業クラスのパフォーマンス、汎用性、密度を提供しますが、これらをエッジに最適化されたコンパクトなフォームファクタで実現しています。

主な機能と利点

- フォームファクタとシャーシ：
 - 1RU 高かつハーフ幅のコンピューティング ノード

- Cisco UCS XE130c M8 コンピューティング ノードは、Cisco UCS XE9305 シャーシに取り付けます
- **CPU** : パフォーマンスコア (P-core) プロセッサを搭載したチップ (SoC) 上の一つの Intel® Xeon® 6 システム (物理コア数 12、20、または 32) 。
- **メモリ** :
 - 合計 8 個の DDR5 DIMM スロット、最大 6400 MT/s RDIMM
 - 8 つの 96 GB DDR5-6400 DIMM で最大 768 GB のメイン メモリ
- **GPU** : ハーフハイト、ハーフレンジス GPU 用の 1 つの専用 PCIe Gen5 GPU スロット。
- **ネットワーク** :
 - シャーシ ミッドプレーンを介して両方の Cisco UCS XE シャーシ管理コントローラの組み込みスイッチに接続する 2 つの統合 25 Gbps ホスト ポート。
 - 2 つの統合 1/10 Gbps RJ45 ホスト ポート。
- **ストレージ** :

Cisco UCS XE130c M8 コンピューティング ノードでは、次の 2 種類のフラッシュストレージ オプションを同時に使用できます。

 - 内部 M.2 SSD : ハードウェア RAID 1 によって保護される最大 2 つの M.2 SSD
 - 前面 E3.S NVMe ドライブ
- **PCIe アダプタ** : ハーフハイト、ハーフレンジス PCIe アダプタ用の 1 つの PCIe Gen5 スロットには、それぞれが最大 15 TB をサポートする 3 台の前面パネルのホットスワップ可能な E3.S NVMe ドライブを含む、IO 最適化構成が必要です。
- **前面パネル インターフェイス** :
 - KVM コネクタ X 1
 - IMC への UART 接続用 USB-C コンソール ポート X 1
- **電源サブシステム** : 電源は Cisco UCS XE9305 シャーシの電源から供給されます。Cisco UCS XE 130c M8 コンピューティング ノードは、最大 425 W を消費します。
- **ファン** : Cisco UCS X9305 シャーシに統合。
- **組み込み管理プロセッサ** :
 - 組み込みの Cisco Integrated Management Controller を使用すれば、Cisco UCS XE130c M8 コンピューティング ノードインベントリ、正常性、およびシステムイベントログを監視することができます。
 - ASPEED AST2600
- **ファームウェア規格** :

- UEFI 仕様 2.9
- ACPI 6.5
- SMBIOS バージョン 3.7
- 前面インジケータ :
 - 電源ボタンおよびインジケータ
 - システム インジケータ
 - ロケーションボタンとインジケータ
- セキュリティ : サーバには、サーバのベースボード管理コントローラ (BMC) に接続されたオンボードのトラステッドプラットフォーム モジュール (TPM) があります。これはセキュアなキーストレージとして機能し、偽造防止を支援します。さらに、サーバは、ホスト システム用にオプションの TPM をサポートしています。

詳細については、「[Cisco UCS XE130c M8 コンピューティング ノード データ シート](#)」および「[Cisco Intersight Unified Edge eCMC インフラストラクチャファームウェア リリース、6.0](#)」を参照してください。

Cisco UCS XE シリーズ M8 サーバーのデバッグ機能テスト

接続セットアップに対応する方法を選択してください。

方法 1 : 直接 USB-C 接続を使用する

USB-C ケーブルをサーバー前面のコンソール ポートに直接接続できます。方法 2 で提供されている詳細な手順は、デバッグ ブレークアウト ケーブルに固有のものであり、この直接接続方法には適用されません。

方法 2 : デバッグ ブレークアウト ケーブル (UCSX-C-DEBUGCBL) を使用する

デバッグ ブレークアウト ケーブル UCSX-C-DEBUGCBL を使用する場合に、サーバ デバッグ機能テストにシリアル ポートを使用するには、次の手順に従います :

1. シリアル ケーブルを接続 :

1. 必要に応じて、DB9 シリアル ケーブルまたは USB からシリアルへのアダプタを使用します。
2. サーバーのシリアルポートからデバッグ コンソールまたはホストシステムにケーブルを接続します。

2. BIOS/UEFI 設定の構成します :

1. 起動時にサーバー BIOS/UEFI にアクセスします。
2. シリアル コンソール リダイレクション オプションを有効にします。
3. ボー レート (通常 115200)、データ ビット (8)、パリティ (なし)、およびストップ ビット (1) を設定します。

3. シリアル ターミナルを起動します :

1. PuTTY、Terra Term、または minicom などの端末エミュレーションツールを使用します。
2. シリアル接続に対応する正しい COM ポートを選択します。
3. BIOS で設定されたボーレートおよびその他のシリアル設定と一致させます。

4. 出力を確認します :

1. サーバを再起動し、シリアル コンソールで POST メッセージとシステム ログを観察します。
2. 必要に応じてシステムを操作できることを確認します(ログイン プロンプトやシェル アクセスなど)。

5. ログおよびキャプチャ :

1. 後で分析するためにデバッグ出力をキャプチャするには、端末ツールでロギングを有効にします。
2. 追跡可能性のためにタイムスタンプを付けてログをパスワード を 変更。

6. トラブルシューティング :

1. 出力が表示されない場合は、ケーブル接続、BIOS 設定、および COM ポートの設定を確認します。
2. 他のサービスやアプリケーションがシリアルポートを占有していないことを確認します。

Cisco UCS X シリーズ M8 サーバファームウェア リリース 6.0(1.252039) の新しいハードウェア

この項では、新しいハードウェア機能について簡単に説明します。

Cisco UCS X580p PCIe ノード

Cisco UCS X580p PCIe ノードは、UCS X シリーズ モジュラー システム向けの最新の PCIe リソース ノードです。生成 AI およびエージェント AI の微調整、推論、および GPU アクセラレーションを必要とするその他のアプリケーションなどのワークロードに対して、高性能な GPU サポートを提供します。

Cisco UCS X580p PCIe ノードは、最大 4 つの PCIe GPU をサポートします。Cisco UCS X210c M8 サーバ (Intel Xeon プロセッサを搭載) または UCS X215c M8 サーバ (EPYC プロセッサを搭載) とペアリングできます。X580p は、GPU 接続に Cisco UCS X-Fabric テクノロジーを使用します。

Cisco UCS X シリーズ M8、M7、M6 6.0(1.250162)、B シリーズ M6、M56.0(1.250157)、および C シリーズ M8、M7、M6 6.0(1.250174) サーバファームウェア リリースで新しいハードウェア：なし

X580p は、X シリーズ シャーシの 2 つの ノード スロットを占有します。ノードごとに最大 4 つの GPU を割り当てられます。各 7RU Cisco UCS X9508 シャーシは最大 2 つの PCIe ノードをサポートします。各ノードは 1 つまたは 2 つのサーバとペアリングします。

詳細については、『[Cisco UCS X580p PCIe ノードのインストールおよびサービス ガイド](#)』および『[Cisco UCS X580p PCIe Node Spec Sheet](#)』を参照してください。

Cisco UCS X9516 X-Fabric

Cisco UCS X9516 X-Fabric は、UCS X9508 シャーシ用の第 2 世代 X-Fabric モジュールです。超低遅延の PCIe Gen5 スイッチングと SmartNIC のサポートにより、柔軟で構成可能な IT リソースが可能になります。Cisco Intersight を介して管理される UCS X9516 X-Fabric では、ポリシーベースの管理を使用してサーバ間で GPU と NIC を動的にプロビジョニングできます。

UCS X580p PCIe ノードと組み合わせることにより、X9516 X-Fabric はノードごとに最大 4 つのデュアルスロット GPU をサポートし、NVLink ブリッジをサポートします。これは、AI 駆動型環境でのモジュラ GPU 構成の制御ポイントとして機能します。

詳細については、『[Cisco UCS X9516 X-Fabric データ シート](#)』を参照してください。

Cisco UCS X580p PCIe ノードおよび Cisco UCS X9516 X-Fabric をサポートするための最小ファームウェア要件

- X580p PCIe ノードファームウェア：6.0(1.252044)
- X9508 シャーシファームウェア：6.0(1.252044)
- Cisco UCS X シリーズ M8 サーバファームウェア：6.0 (1.252039)
- ファブリック インターコネクト インフラストラクチャファームウェア：6.0(1.250229)



(注) X580p PCIe ノードファームウェア 6.0(1.252044) および X9508 シャーシファームウェア 6.0(1.252044) は、個別のバンドルとして利用できます。

Cisco UCS X シリーズ M8、M7、M6 6.0(1.250162)、B シリーズ M6、M56.0(1.250157)、および C シリーズ M8、M7、M6

6.0(1.250174) サーバファームウェア リリースで新しいハードウェア：なし

Cisco UCS X シリーズ M8、M7 6.0(1.250122)、M6、B シリーズ M66.0(1.250127)、M56.0(1.250131) および C シリーズ M8、M7、M6 サーバファームウェア リリースの新しいハードウェア：なし

Cisco UCS X シリーズ M8、M7、M6 6.0(1.250120) および C シリーズ M8、M7、M6 6.0(1.250127) サーバファームウェア リリースの新しいハードウェア

- Cisco UCS C225 M8 サーバーで 30TB 2.5 インチ QLC ドライブをサポートします
- Cisco UCS C シリーズ M8 および C240L M6 サーバーで、次世代の大型フォーム ファクタ (3.5 インチ) ハードディスク ドライブをサポートします。
- Cisco UCS C240 M8 サーバー上の Cisco トライモード M1 24GRAID (UCSC-RAID-M1L16) コントローラのデュアルサポート、同じサーバー環境内の 2 つのコントローラの独立した構成と管理を可能にします。
- インフラファームウェア リリース 6.0 (1) 以降、Cisco UCS X シリーズおよび C シリーズサーバーは Cisco UCS 6664 ファブリック インターコネクトをサポートします。

詳細については、「[Cisco Intersight 管理モードインフラストラクチャファームウェア、リリース 6.0 のリリースノート](#)」を参照します。

Cisco UCS X シリーズ M8、M7、M6 6.0(1.250120) および C シリーズ M8、M7、M6 6.0(1.250127) サーバー ファームウェア リリースの新しいハードウェア



第 4 章

セキュリティ修正

Cisco バグ検索ツールを使用して、未解決の問題、解決済みの問題、およびセキュリティ修正を表示できます。

- Cisco UCS X シリーズ M8、M7、M6 6.0(2.260069)、C シリーズ M8、M7、M6 6.0(2.260069)、および B シリーズ M6 6.0(2.260069) サーバー ファームウェア リリース (26 ページ)
- Cisco UCS B シリーズ M5 サーバー ファームウェア リリース 6.0(1.260012) のセキュリティフィックス (26 ページ)
- Cisco UCS X シリーズ M8、M7、M6 6.0(2.260040)、XE シリーズ M8 6.0(2.260042)、C シリーズ M8、M7、M6 6.0(2.260044)、および B シリーズ M6 6.0(2.260040) サーバー ファームウェア リリースのセキュリティ修正 (27 ページ)
- XE シリーズ M8 サーバファームウェア リリース 6.0(1.260001) のセキュリティ修正：なし (48 ページ)
- C シリーズ M8 サーバファームウェア リリース 6.0(1.250194) のセキュリティ修正：なし (48 ページ)
- Cisco UCS X シリーズ M8、M7 6.0(1.252114)、M6、B シリーズ M66.0(1.250179)、M56.0(1.250169) および C シリーズ M8、M7、M6 6.0(1.250192) サーバファームウェア リリースでセキュリティ修正：なし (48 ページ)
- XE シリーズ M8 6.0(1.251030) サーバファームウェア リリースのセキュリティ修正：なし (48 ページ)
- X シリーズ M8 サーバファームウェア リリース 6.0(1.252039) のセキュリティ修正：なし (48 ページ)
- C シリーズ M8、M7、M6 6.0(1.250174) サーバファームウェア リリースのセキュリティ修正 (48 ページ)
- Cisco UCS X シリーズ M8、M7、M6 6.0(1.250122)、B シリーズ M6、M5 6.0(1.250127) および C シリーズ M8、M7、M6 6.0(1.250131) サーバー ファームウェア リリース：なし (50 ページ)
- Cisco UCS X シリーズ M8、M7、M6 6.0(1.250120)、B シリーズ M6、M5 6.0(1.250126) および C シリーズ M8、M7、M6 6.0(1.250127) サーバー ファームウェア リリース (50 ページ)

Cisco UCS X シリーズ M8、M7、M6 6.0(2.260069)、C シリーズ M8、M7、M6 6.0(2.260069)、および B シリーズ M6 6.0(2.260069) サーバー ファームウェア リリース

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 ID	説明
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。

Cisco UCS B シリーズ M5 サーバー ファームウェア リリース 6.0(1.260012) のセキュリティ フィックス

Defect ID - [CSCwq34278](#)

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 ID	説明
CVE-2025-20064	特定の Intel リファレンス プラットフォーム上の UEFI FlashUcAcmSmm モジュールでの不適切な入力検証により、権限を持つローカルの攻撃者が任意のコードを実行して権限を昇格させ、システムの機密性、完全性、および可用性に深刻な影響を与える可能性があります。

CVE ID	説明
CVE-2025-20027	特定の Intel リファレンス プラットフォーム上の UEFI WeaERSST モジュールでの不適切な入力検証、特権を持つローカルの攻撃者が権限をエスカレーションし、システムの機密性、完全性、および可用性に影響を与える可能性があります。
CVE-2025-20028	特定の Intel リファレンス プラットフォームの UEFI WhaERST SMM モジュールにおけるチェック時 (TOCTOU) の競合状態により、権限を持つローカルの攻撃者が権限をエスカレーションし、システムの機密性、完全性、および可用性に影響を与える可能性があります。
CVE-2025-20105	Intel リファレンス プラットフォーム上の特定の UEFI ファームウェア SMM モジュールにおける不適切な入力検証により、特権を持つローカルの攻撃者が複雑度の低い任意のコードを実行し、システムの機密性、完全性、および可用性に大きな影響を与え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。

Cisco UCS X シリーズ M8、M7、M6 6.0(2.260040)、XE シリーズ M8 6.0(2.260042)、C シリーズ M8、M7、M6 6.0(2.260044)、および B シリーズ M6 6.0(2.260040) サーバー ファームウェア リリース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 (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 ID	説明
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 ID	説明
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。

不具合 ID: CSCwr81218

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 ID	説明
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

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 ID	説明
CVE-2021-0920	Linux カーネルの Unix ドメイン ソケット実装 (unix_scm_to_skb_inaf_unix.c) 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 ID	説明
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 タイマー処理において、handle_posix_cpu_timers() 関数と posix_cpu_timer_del() 関数の間で競合状態（レースコンディション）が発生し、Use-After-Free（解放後使用）の状態を招く可能性があります。これにより、ローカルユーザーが権限を昇格させたり、システムをクラッシュさせたりする恐れがあります。

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: [CSCws61975](#)

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 ID	説明
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](#)

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 ID	説明
CVE-2010-2252	Wget 1.12 以前では、-O（出力先指定）オプションの使用時に、元の URL ではなくリダイレクト先の URL に含まれるファイル名が使用されるため、異なるファイル名を持つ URL への 302 リダイレクトを介して、リモートの攻撃者が任意のファイルに書き込みを行うことが可能です。
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	1.18 より前の Wget では、リモート サーバーは、FTP URL に HTTP 要求を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 サーバーによって指定された名前でファイルを保存します。
CVE-2017-6508	1.19.1 より前の Wget 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（CRLInjection）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	1.19.5 より前の Wget 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	1.21.1 より前の Wget 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る。
CVE-2024-38428	1.24.5 より前の Wget には、URI のユーザー情報を適切に解析しないという欠陥に対する脆弱があり、特定の設定でセキュリティフィルタをバイパスたり、ログイン情報の漏洩につなが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

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 ID	説明
CVE-2009-5155	GNU C ライブラリ (glibc) の <code>strfmon_l</code> 関数の off-by-1 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、大きな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 <code>tar</code> の実装では、リモートの攻撃者が <code>tar</code> 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ようになります。
CVE-2012-4412	GNU C ライブラリ (glibc) の <code>strcoll</code> 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 <code>strcoll</code> 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 <code>read_dir_r</code> 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 <code>getaddrinfo</code> 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 <code>posix_spwn_file_actions_addopen</code> 関数は、その <code>path</code> 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 ID	説明
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 関数を使用すると、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 関数における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は、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 resquery 関数での NULL ポインタ逆参照により、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 関数で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することができます。
CVE-2015-8778	GNU C ライブラリ (glibc) の hcreate 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、多数の要素を介して、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 ID	説明
CVE-2015-8779	GNU C ライブラリ (glibc) の <code>catopen</code> 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 <code>strftime</code> 関数で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 <code>_IO_wstr_overflow</code> 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、大きな文字列を介して、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-2015-8984	GNU C ライブラリ (glibc) の <code>fnmatch</code> 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 <code>pop_fail_stack</code> 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 <code>iconv</code> 関数における範囲外への書き込みにより、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、細工されたマルチバイトシーケン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-2016-10739	GNU C ライブラリ (glibc) の <code>getaddrinfo</code> 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 <code>AF_INET6</code> 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 <code>glob</code> 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 <code>getnetbyname</code> 関数における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 ID	説明
CVE-2016-3706	GNU C Library (glibc) の <code>getaddrinfo</code> 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 <code>hostent</code> 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 <code>clntudp_call</code> 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 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 <code>glob</code> 関数の <code>off-by-1</code> 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する。
CVE-2017-15671	2.27 より前の GNU C ライブラリ (glibc) の <code>glob</code> 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 <code>elf/dl-load.c</code> 実装は、特定のチェックを適切に処理しないため、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 <code>memmove</code> と <code>memcpy</code> 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。そのため、コンテキスト依存の攻撃者が、サービス拒否（クラッシュ）を引き起こす可能性があります。また、特定できないその他の影響を及ぼす可能性もあります。
CVE-2018-1000001	GNU C ライブラリ (glibc) の <code>realpath</code> 関数でのバッファアンダーフローにより、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-2018-11236	GNU C ライブラリ (glibc) の <code>vfprintf_internal</code> 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、大きな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 ID	説明
CVE-2018-6485	GNU C ライブラリ (glibc) 2.26 以前の <code>posix_memalign</code> 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、ヒープの破損につながる可能性があります。
CVE-2019-1010023	GNU C ライブラリ (glibc) の <code>ld.so</code> 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、ローカルの攻撃者は、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 <code>LD_PRELOAD</code> 環境変数を適切に処理しないため、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 <code>iconv</code> 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-2019-9169	GNU C ライブラリ (glibc) の <code>regcomp</code> 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 <code>cosl</code> 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、大きな入力値を介して、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-2020-1751	GNU C ライブラリ (glibc) の <code>dl_open</code> 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 <code>glob</code> 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は、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 <code>iconv</code> 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 ID	説明
CVE-2020-29573	GNU C ライブラリ (glibc) の printf 関数でバッファ オーバーフローが発生し、コンテキスト依存の攻撃者が大きな精度の値を介してサービス拒否 (クラッシュ) を引き起こす可能性があります。
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) におけ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-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 関数でバッファ 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) を引き起こす可能性があります。
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、ローカルの攻撃者は、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 関数における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-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きな 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 ID	説明
CVE-2023-4813	GNU C ライブラリ (glibc) の <code>getaddrinfo</code> 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 <code>ld.so</code> 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 <code>getaddrinfo</code> 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 <code>iconv</code> 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-2024-33599	GNU C ライブラリ (glibc) の <code>nscd</code> (ネーム サービス キャッシュ デモン) 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 <code>nscd</code> (ネーム サービス キャッシュ デモン) 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 <code>nscd</code> (ネーム サービス キャッシュ デモン) 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 <code>nscd</code> (ネーム サービス キャッシュ デモン) 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 から 2.40 の <code>assert ()</code> 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 ID	説明
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、悪意のある共有ライブラリをロードし、静的にコンパイルされた <code>setuid</code> バイナリ内の <code>dlopen</code> を呼び出す信頼できない <code>LD_LIBRARY_PATH</code> を介して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 プロセッサ用に最適化された <code>strcmp</code> 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 <code>regcomp</code> 関数でのダブルフリーの脆弱性は、メモリ割り当て障害が発生した場合にブラケットの解析中に発生し、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 : [CSCws68836](#)

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 ID	説明
CVE-2007-5116	Perl 5.8 の正規表現エンジン (<code>regcomp.c</code>) のポリモーフィック型イック 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することが可能になります。
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 <code>File::Path</code> の <code>rmtree</code> 関数の競合状態により、ローカル ユーザーがシンボリックリンク攻撃を介して任意の <code>setuid</code> バイナリを作成できる。
CVE-2008-5303	Perl 5.8.8 の <code>File::Path</code> の <code>rmtree</code> 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るようになります。

CVE ID	説明
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-2010-1447	Perl 用の 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、サブルート参照や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、HTTP 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により、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 Digest 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、「x」文字列のリピート演算子を介してサービス拒否を引き起こしたり、任意のコードを実行したりできるようになります。

CVE ID	説明
CVE-2012-5526	Perl 用の 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 より前および 5.24.1）は、モジュール包含パス（@INC）からカレントディレクトリ（「.」）を適切に削除しないため、ローカルユーザは、トロイの木馬モジュールを介して権限を取得できます。
CVE-2016-2381	Perl は、コンテキスト依存の攻撃者が、envp 配列の重複した環境変数を使用し、子プロセスの汚染保護メカニズムをバイパスさせる可能性があります。
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、ローカルユーザが悪意のあるライブラリを介して任意のコードを実行できる可能性があります。
CVE-2018-12015	Perl 5.26.2 までの Archive::Tar モジュールのため、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できます。

CVE ID	説明
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 <code>pack</code> 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は、大きな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 (<code>regcomp.c</code>) では、 <code>S_study_chunk</code> の再帰的呼び出し中に、バッファ オーバーフローの脆弱性が発生します。
CVE-2020-16156	CPAN 2.28 では、署名検証の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 <code>tr</code> 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	Perl スレッドにおけるディレクトリ ハンドル複製時の競合状態により、現在の作業ディレクトリが予期せず変更される可能性があります。これにより、ローカル攻撃者がスレッドに悪意のあるコードを読み込ませるよう仕向ける恐れがあります。影響を受けるサードパーティ製ソフトウェアコンポーネントは、この脆弱性への修正を含むバージョンに更新されました。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](#)

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 ID	説明
CVE-2025-27363	FreeType バージョン 2.13.0 以下の範囲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 subglyph 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](#)

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 ID	説明
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時に 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ると発生し、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。

Defect ID - [CSCwq11344](#)

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 ID	説明
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ます、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 to/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 ID	説明
CVE-2010-1151	Apache HTTP サーバの <code>mod_auth_shadow</code> 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 <code>mod_macro</code> 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	<code>mod_http2</code> 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 サーバは、単一ストリーム内で送信される HTTP/2 CONTINUATION 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 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-Side 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 ID	説明
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 Apache HTTP 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 ハッシュが漏洩され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、OIDCPreservePost 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](#)

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 ID	説明
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したり、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イックオPCODE 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 文字に切り替えることで任意のコードを実行することが可能になります。
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 <code>bsd_glob</code> 関数により、コンテキスト依存の攻撃者は <code>GLOB_ALTDIRFUNC</code> フラグを使用した <code>glob</code> 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 <code>decode_xs</code> 関数の <code>off-by-one</code> 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 <code>Locale::Maketext</code> 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 <code>Data::Dumper</code> の <code>Dumper</code> 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 <code>Array-Reference</code> 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 ID	説明
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 より前および 5.24.1）は、モジュール包含パス（@INC）からカレントディレクトリ（「.」）を適切に削除しないため、ローカルユーザは、トロイの木馬モジュールを介して権限を取得できます。
CVE-2016-2381	Perl は、コンテキスト依存の攻撃者が、envp 配列の重複した環境変数を使用し、子プロセスの汚染保護メカニズムをバイパスさせる可能性があります。
CVE-2017-12814	Windows の 5.24.3-RC1 より前の 5.26.x および 5.26.1-RC1 より前の Perl の CPerlHost::Add メソッドの CPerlHost::Add メソッドにより、攻撃者が長い環境変数を介して任意のコードを実行できるを参照してください。
CVE-2017-12837	5.24.3-RC1 より前、および 5.26.1-RC1 より前の 5.26.x の Perl 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のため、リモートの攻撃者は、\N{} エスケープと、case-insensitive 修飾子を含む正規表現を用いて、サービス拒否状態を引き起こす可能性があります。
CVE-2017-12883	5.24.3-RC1 より前、および 5.26.1-RC1 より前の 5.26.x の Perl における、regcomp.c の S_grok_bslash_N 関数のバッファオーバーフローにより、リモートの攻撃者は、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を用いて、機密情報を開示したり、サービス拒否状態を引き起こす可能性があります。
CVE-2018-12015	Perl 5.26.2 までの Archive::Tar モジュールのため、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できます。
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 ID	説明
CVE-2018-18313	Perl 5.26.3 および 5.28.1 より前の <code>regcomp.c</code> の <code>S_grok_bslash_N</code> 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 <code>regcomp.c</code> の <code>S_regtom</code> 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 <code>pack</code> 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は、大きな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 (<code>regcomp.c</code>) では、 <code>S_study_chunk</code> の再帰的呼び出し中に、バッファオーバーフローの脆弱性が発生します。
CVE-2022-48522	警告メッセージを出力しようとする、Perl 5.34.0 の <code>S_find_uninit_var</code> 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、ユーザが中間者攻撃にさらされます。
CVE-2023-31486	Perl のコアモジュールである HTTP::Tiny の 0.083 より前には、安全でないデフォルト TLS 設定があつて、ユーザが証明書の検証をオプトインする必要があり、そのため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	Windows の Perl には、バイナリハイジャックの脆弱性があります。これは、システムパスに依存してシェル (<code>cmd.exe</code>) 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。

XE シリーズ M8 サーバファームウェア リリース 6.0(1.260001) のセキュリティ修正：なし

C シリーズ M8 サーバファームウェア リリース 6.0(1.250194) のセキュリティ修正：なし

Cisco UCS X シリーズ M8、M7 6.0(1.252114)、M6、B シリーズ M6 6.0(1.250179)、M5 6.0(1.250169) および C シリーズ M8、M7、M6 6.0(1.250192) サーバファームウェア リリースでセキュリティ修正：なし

XE シリーズ M8 6.0(1.251030) サーバファームウェア リリースのセキュリティ修正：なし

X シリーズ M8 サーバファームウェア リリース 6.0(1.252039) のセキュリティ修正：なし

C シリーズ M8、M7、M6 6.0(1.250174) サーバファームウェア リリースのセキュリティ修正

このセクションでは、セキュリティ修正について簡単に説明します。

不具合 ID - CSCwq36167

Cisco UCS C-Series M6 ラック サーバーは、次の一般的な脆弱性およびエクスポージャ（CVE）ID によって特定された脆弱性の影響を受けるインテル CPU を搭載しています：

- **CVE-2025-20067**：一部の Intel（R）CSME および Intel（R）SPS ファームウェアに観察可能なタイミングの不一致があるため、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効に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 - CSCwq36171

Cisco UCS C-Series M7 ラック サーバーは、次の一般的な脆弱性およびエクスポージャ（CVE）ID によって特定された脆弱性の影響を受けるインテル CPU を搭載しています。

- **CVE-2025-21096**：一部の Intel（R）TDX のファームウェアの不適切なバッファ制御により、権限ユーザーがローカルアクセスを介して権限のエスカレーションを有効にできる可能性があります。
- **CVE-2025-20053**：一部の Intel（R）Xeon（R）プロセッサの SGX 対応ファームウェアの不適切なバッファ制御により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2025-24305**：一部の Intel（R）Xeon（R）プロセッサの Alias Checking Trusted Module（ACTM）ファームウェアの制御フロー管理が不十分なため、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効にできる可能性があります。
- **CVE-2025-20613**：一部の Intel（R）TDX 向けファームウェアの疑似乱数生成器（PRNG）の予測シードで、認証されたユーザーがローカルアクセスを介した情報開示を有効にする可能性があります。
- **CVE-2025-21090**：一部の Intel（R）Xeon（R）プロセッサにアクティブに割り当てられたリソースへの参照が見つからない場合、認証されたユーザーがローカルアクセスを介してサービス拒否を有効にする可能性があります。
- **CVE-2025-22853**：一部の Intel（R）TDX のファームウェアの不適切な同期により、特権ユーザーがローカルアクセスを介して特権のエスカレーションを有効に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。

Cisco UCS X シリーズ M8、M7、M6 6.0(1.250122)、B シリーズ M6、M5 6.0(1.250127) および C シリーズ M8、M7、M6 6.0(1.250131) サーバー ファームウェア リリース：なし

Cisco UCS X シリーズ M8、M7、M6 6.0(1.250120)、B シリーズ M6、M5 6.0(1.250126) および C シリーズ M8、M7、M6 6.0(1.250127) サーバー ファームウェア リリース

このセクションでは、セキュリティ修正について簡単に説明します。

不具合 ID - CSCwm98102

Cisco UCS B シリーズ ブレード サーバー、UCS C シリーズ ラック サーバー、UCS X シリーズ コンピューティング ノードには、以下の共通脆弱性識別子 (CVE) ID で識別される脆弱性の影響を受ける、オプションの Trusted Platform Module (TPM) 2.0 が含まれています：

- **CVE-2025-2884** : TCG TPM2.0 リファレンスの実装の CryptHmacSign ヘルパー関数は、署名キーのアルゴリズムで署名スキームの検証が不足しているため、境界外読み取りに対して脆弱です。TCG 標準規格 TPM2.0 については、エラッタ リビジョン 1.83 およびアドバイザリ TCGVRT0009 を参照してください。

Cisco UCS サーバーには、次のオプション TPM モジュールのいずれかが搭載されています。

- UCSX-TPM2-002
- UCSX-TPM-002C
- UCS-TPM-002D
- UCSX-TPM-002D

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。



第 5 章

解決済みの問題

Cisco バグ検索ツールを使用して、未解決の問題、解決済みの問題、およびセキュリティ修正を表示できます。

- Cisco UCS X シリーズ M8、M7 6.0(2.260069) および C シリーズ M8 6.0(2.260069) サーバファームウェア リリースの解決済みの問題 (52 ページ)
- B シリーズ M5 サーバファームウェア リリース 6.0(1.260012) の解決済みの問題 (54 ページ)
- Cisco UCS X シリーズ M8、M7、M6 6.0(2.260040)、XE シリーズ M8 6.0(2.260042)、C シリーズ M8、M7、M6 6.0(2.260044)、および B シリーズ M6 6.0(2.260040)サーバファームウェア リリースの解決済みの問題 (54 ページ)
- XE シリーズ M8 サーバファームウェア リリース 6.0(1.260001) の解決済みの問題 (58 ページ)
- C シリーズ M8 サーバファームウェア リリース 6.0(1.250194) の解決済みの問題：なし (60 ページ)
- Cisco UCS X シリーズ M7 6.0(1.250179) および C シリーズ M7、M6 6.0(1.250192) サーバファームウェア リリースの解決済みの問題 (60 ページ)
- XE シリーズ M8 サーバファームウェア リリース 6.0(1.251030) の解決済みの問題：なし (61 ページ)
- X シリーズ M8 サーバファームウェア リリース 6.0(1.252039) の解決済みの問題：なし (61 ページ)
- Cisco UCS X シリーズ M8 6.0(1.250162) および C シリーズ M8、M6 6.0(1.250174)サーバファームウェア リリースの解決済みの問題 (61 ページ)
- Cisco UCS X シリーズ M8、M7 6.0(1.250122)、M6、B シリーズ M6、M56.0(1.250127) および C シリーズ M8、M7、M6 6.0(1.250131)サーバファームウェア リリースの解決済みの問題 (65 ページ)
- Cisco UCS C シリーズ M8、M7 および M6 6.0(1.250127)サーバファームウェア リリースで解決された不具合 (66 ページ)

Cisco UCS X シリーズ M8、M7 6.0(2.260069) および C シリーズ M8 6.0(2.260069) サーバファームウェア リリースの解決済みの問題

ここでは、解決済みの問題について簡単に説明します。

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwt34870	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 サーバーでは、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) サービスが応答なくなり、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。	C シリーズ : 6.0 (2.260044)	C シリーズ : 6.0(2.260069)

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwt18924	アップストリーム Cisco ACI ファブリックのアップグレードまたはリロード後、Cisco UCS VIC アダプタが vNIC をオンラインにできない場合があります。アダプタの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。アダプタログにアダプタでメモリ不足状態が発生していることが示され、その後リセットが行われる場合があります。この問題は、Cisco UCS VIC 1400 シリーズおよび 15000 シリーズアダプタの 10GBase-T (10G-TX) トランシーバで観察され、トランシーバが I2C バスを保持している場合、スイッチまたはサーバのリロードイベント中にトリガーされ、アダプタのメモリリークの原因となる可能性があります。 この問題は解決されました。	C シリーズ : 4.3(5.250030)	C シリーズ : 6.0(2.260069)
CSCwt42347	ホストファームウェアパッケージ (HFP) をリリース 4.3 (2) から 6.0 (2) にアップグレードする際、UCSX-X10C-RAIDF コントローラを搭載した Cisco UCS X シリーズサーバでは、ハードウェア構成を確認するための準備の段階で障害が発生し、結果としてユニファイド BIOS 管理 (UBM) アップグレードがハングします。ファームウェアの更新プロセスが完了せず、BMC ログには更新プロセスが無限に実行されていることが示されます。 この問題は解決されました。	X シリーズ:6.0 (2.260040)	X シリーズ : 6.0(2.260069)

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwt35920	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。 この問題は解決されました。	X シリーズ : 6.0 (2.260040) C シリーズ : 6.0 (2.260044) X580p PCIe ノード : 6.0 (2.260043)	X シリーズ : 6.0(2.260069) C シリーズ : 6.0(2.260069) X580p PCIe ノード : 6.0(2.260069)

B シリーズ M5 サーバファームウェア リリース 6.0(1.260012) の解決済みの問題

ここでは、解決済みの問題について簡単に説明します。

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwr21671	Windows Server 2019 (Megafas2 ドライバ) を実行する LSI 12G RAID コントローラを搭載した Cisco UCS B200 M5 サーバでは、RAID コントローラで L2/L3 キャッシュエラーが検出される場合があります。これにより、ストレージコントローラが動作不能になり、Cisco IMC はコントローラを検出できなくなります。 この問題は解決されました。	4.2 (3e)	5.4(0.260011) 6.0(1.260012)

Cisco UCS X シリーズ M8、M7、M6 6.0(2.260040)、XE シリーズ M8 6.0(2.260042)、C シリーズ M8、M7、M6 6.0(2.260044)、および B シリーズ M6 6.0(2.260040) サーバファームウェア リリースの解決済みの問題

ここでは、解決済みの問題について簡単に説明します。

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
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の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 入力を受け入れられません。 この問題は解決されました。	X シリーズ M7:5.4 (0.250048) C シリーズ M7:4.3 (6.250053)	X シリーズ M7 : 6.0(2.260040) C シリーズ M7 : 6.0(2.260044)
CSCwb62117	Brocade SAN スイッチと Dell storage 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)
CSCwr51315	Cisco UCS X シリーズ サーバで、NVMe ドライブ (ファームウェア E2CS005 の UCS -NVMEG4-M7680) は、予想される Cisco SSID 4800 ではなく SSID 5000 を表示します。この不一致により、コンプライアンスチェックが失敗し、ディスクが「unclaimed (未要求)」としてマークされます。 この問題は解決されました。	6.0(1.250120)	6.0(2.260040)

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwr73352	複数の Cisco UCS X210c M7 サーバで、BMC ウォッチドッグのハードリセットによってトリガーされた Cisco IMC の再起動が発生します。これにより、再起動中にサービスプロファイルに一時的にアクセスできなくなります。この動作は、リセットイベント中のサーバ管理の可用性に影響を与える可能性があります。この問題は解決されました。	5.2(1.240010)	6.0(2.260040)
CSCwq55604	すべての Cisco UCS C245 M8 統合サーバの DIMM_P2_H1 が動作不能として報告されますが、実際にはすべての DIMM がメモリ エラーなく正常に機能します。この問題は、サーバがサポートされている同一の DIMM モデルをフルに装着しているにもかかわらず、機器の動作不能とサーバファームウェアの非互換性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)
CSCwq17020	UCSX-X10C-RAIDF コントローラの背後に 3.8TB 以上の容量の U3 Micron ドライブを JBOD モードで取り付けした後、EFI ブートイメージのロードに関連する BIOSerrors が原因で Linux OS が起動に失敗します。この問題は、特に Intel® プロセッサを搭載した Cisco UCS X シリーズ M8 サーバで発生し、複数の Linux ディストリビューションに影響します。ドライブが RAID0 で構成されている場合、問題は発生しません。より小さい容量のドライブを使用している場合、または RAID0 を使用している場合、Microsoft Windows® および Linux OS は正常に起動します。この問題は解決されました。	X210c:5.4 (0.250037) X215c:5.4 (0.250035)	6.0(2.260040)

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwr82017	Cisco UCS X210c M8、C220 M8、および C240 M8 サーバでは、IntelSGX を有効にし、システムメモリ設定でプロセッサ予約済みメモリ範囲レジスタ (PRMRR) サイズをサポートされていない値に設定すると、システムが継続的に再起動します。サポートされていないサイズが構成された時のみにこの問題が発生します。 この問題は解決されました。	X シリーズ M8:6.0 (1.252114) C シリーズ M8 : 6.0 (1.250192)	X シリーズ M8 : 6.0(2.260040) C シリーズ M8 : 6.0(2.260044)
CSCwr82475	Cisco Unified Edge サーバー UCSXE-130C-M8 において、UEFI セキュアブートモードでファームウェアをバージョン 6.0 (1.250003) から 6.0 (1.251026) にアップグレードした後、タイミングや競合状態 (レース コンディション) に起因して、BMC ブート時に FIT4 レコードをセカンダリ サービス プロセッサ (SSP) へ転送する処理が失敗する場合があります。これにより、必要な認証ハンドシェイクが防止され、ホストシステムの POST がハングします。 BIOS POST の完了の失敗 エラーが表示され、次のようなメッセージがログに記録されます。 • peci command(0xa1) failed: 0x63 • peci rdpkgconfig command (0xa1) failed (result code: 0x63, addr: 0x30) • ast2600-ssp ahb:secondary-service-processor: Kicking SSP vqid = 1 回避策 : 問題を解決するために BMC を再起動します。	XE シリーズ M8 : 6.0 (1.250003)	XE シリーズ M8 : 6.0(2.260042)

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwr05911	Cisco Unified Edge サーバでは、ホストの電源がオフになると、IMM インベントリ ページには、eCMC:A で LOM- NIC-1 インターフェイスが eCMC:B でアップとして表示されますが、eCMC:B では asdown と表示されます。この不整合は、ホストの電源がオフの場合にのみ発生します。この問題による機能への影響はありません。 この問題は解決されました。	XE シリーズ M8 : 6.0 (1.251030)	XE シリーズ M8 : 6.0(2.260042)
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。	C シリーズ : 4.3 (6.260017) B シリーズ : 5.4 (0.260011)	C シリーズ : 6.0(2.260044) B シリーズ : 6.0(2.260040)

XE シリーズ M8 サーバ ファームウェア リリース 6.0(1.260001) の解決済みの問題

ここでは、解決済みの問題について簡単に説明します。

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwb24234	Cisco UCS XE130c M8 コンピューティング ノードでは、UCS-M2-HWRAID MINI STOR コントローラが見つからないが、そのキャリアがインストールされている場合、システム ログが unable to read fru information エラーで継続的にフラッシュします。 ファームウェアをアップグレードすると、問題が解決します。 アップグレード後も同じエラーが続く場合は、M.2 コントローラとそのキャリアの両方が正しく装着され、取り付けられていることを物理的に確認します。	6.0 (1.251030)	6.0(1.260001)
CSCws22743	Cisco UCS XE130c サーバーでは、L4/L40S GPU で、競合状態が原因で x8 幅および GEN 1 速度へのリンク ダウングレードが発生する場合があります。これは、GPU のパフォーマンスを低下させる可能性があり、通常は、リンクがダウングレードされたり、レーンの幅が縮小された場合に発生します。 リンク ダウングレードから回復するために、デバイスを通常の動作に戻すという回避策が導入されました。	6.0 (2.250123)	6.0(1.260001)

C シリーズ M8 サーバファームウェア リリース 6.0(1.250194) の解決済みの問題：なし

Cisco UCS X シリーズ M7 6.0(1.250179) および C シリーズ M7、M6 6.0(1.250192) サーバファームウェア リリースの解決済みの問題

ここでは、解決済みの問題について簡単に説明します。

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCws30219	Cisco UCS M7 サーバは、ECC（エラー訂正コード）メモリイベントによってトリガーされたホストロックアップの影響を受けます。 これは、エラー状態時にサーバの BIOS が EFI（Extensible Firmware Interface）と通信する仕組みに特に関連しています。これらのイベント中、BIOS は必要な変数を正しく取得せず、EFI は無効なパラメータを返します。その結果、オペレーティングシステムは通常の動作を続行できず、エラーをログに記録せずにフリーズします。これが発生すると、ホストは応答しなくなり、KVM（キーボード、ビデオ、マウス）入力は受け入れられません。 シングルビット ECC エラー（DDR5 仕様によりログは記録されません）がこの状態をトリガーする可能性があり、その結果、ホストの応答性が完全に失われます。	X シリーズ M7:5.4 (0.250048) C シリーズ M7:4.3 (6.250053)	X シリーズ M7 : 6.0(1.250179) C シリーズ M7 : 6.0(1.250192)

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwi71153	Cisco UCS C シリーズ M6 サーバでは、カーネルスケジューラの null ポインタの逆参照によって引き起こされたウォッチドッグリセットが原因で、BMC リセットが発生します。 さらに、サーバでカーネルパニックが発生する場合があります。	4.2(3b)	C シリーズ M6 : 6.0(1.250192)

XE シリーズ M8 サーバファームウェア リリース 6.0(1.251030) の解決済みの問題：なし

X シリーズ M8 サーバファームウェア リリース 6.0(1.252039) の解決済みの問題：なし

Cisco UCS X シリーズ M8 6.0(1.250162) および C シリーズ M8、M6 6.0(1.250174)サーバファームウェア リリースの解決済みの問題

ここでは、解決済みの問題について簡単に説明します。

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwq61388	CIMC 4.3.5 以降を実行している Cisco UCS C シリーズ M6 サーバーで、複数の NVMe ドライブがある状態で BIOS の VMD を有効にすると、ストレージ サブシステムの初期化が 15 分を超え、Intersight サーバー プロファイルの展開が失敗する可能性があります。 この問題が発生する可能性は、取り付けられているドライブの数が増えると増加します。 VMD を無効にするか、ドライブの数を減らすと、問題を解決できます。	4.3(5.250001)	6.0(1.250162) 6.0(1.250174)
CSCwq74490	AMD EPYC 9655 プロセッサを搭載した Cisco UCS C245 M8 プラットフォームにおいて、NVIDIA L4 GPU をフル構成で搭載し、Linux Rebooter ストレステストを実行すると、異なるスロットでランダムに PCIe リンク幅が低下する現象が発生します。AC 電源の再投入や HUU の更新などのアクション後に、影響を受けるスロットが変更された。たとえば、最初にスロット 2 および 6 がダウングレードされた場合、これらのアクション後に他のスロットがダウングレードされる可能性があります。これにより、OS 環境で GPU の動作速度が低下する可能性があります。	4.3(6.250053)	6.0(1.250162) 6.0(1.250174)

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwq01863	スタンドアロン モードの Cisco UCS C225 または C245 M8 サーバでは、636 以外のポートでセキュア LDAP (LDAPS) を構成すると、サーバはセキュアではなく標準規格の LDAP 接続を試行し、LDAPS 認証が失敗します。 セキュアな LDAP 接続には常にポート 636 を使用します。他のポートは LDAPS では動作しません。	4.3(6.250044)	6.0(1.250162) 6.0(1.250174)
CSCwr24516	Cisco UCS X210c M8 では、特定のベンダーのハードウェア部品（インダクタ）が含まれている場合、一部のサーバーの電源がオンにならないか、または起動しない場合があります。この問題により、スタートアップに失敗し、サーバーの電源を入れようとしてもオフのままになります。この問題は、新しいハードウェア部分の動作の違いによって発生しますが、この新しいコンポーネントをサポートするように設計された最新の VR（電圧レギュレータ）イメージにボードを更新することで、完全に解決できます。 最新の VR イメージでサーバーを更新し、電源投入時のエラーをクリアして、サーバーの電源をオフにしてから再度オンにします。それでもサーバーが起動しない場合は、Cisco TAC に連絡してサポートを受けてください。	6.0(1.250126)	6.0(1.250162) 6.0(1.250174)

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwp91696	Cisco UCS X215c M8 サーバでは、サーバがすでに実行されているときに E3.SNVMe ドライブを空のスロットに追加すると、ドライブは第 5 世代ではなく第 4 世代の速度で接続します。この問題は、起動中にスロットが空であり、オペレーティングシステムの起動後にドライブがホット挿入された場合にのみ発生します。 サーバーの電源を入れる前に、ドライブをスロットに挿入します。後から追加されたドライブは、サーバーが再起動されるまで第 4 世代の速度でのみ動作します。	6.0 (1.250065)	6.0(1.250162) 6.0(1.250174)
CSCwq01510	Cisco UCS X215c-M8 サーバーでは、オペレーティングシステムの起動時にこれらのスロットが空だった場合、スロット 8 またはスロット 9 の E3.SNVMe ドライブのホットプラグは ESXi または Windows で機能しません。起動後に追加または削除されたドライブは、OS によって検出されません。 回避策はありません。OS の起動中にスロット 8 とスロット 9 が空の場合、ホットプラグは機能しません。	6.0 (1.250086)	6.0(1.250162) 6.0(1.250174)

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwd93635	CIMC 4.3.5 以降のファームウェアを実行している Cisco UCS C240 M6 サーバでは、多数の NVMe ドライブと VMD が BIOS で有効になっている場合、ストレージサブシステムの初期化時間が長くなり、最大 50 分かかる場合があります。この遅延により、Intersight Server Profile のワークフローにおいて、特に「BIOS POST 完了の待機」ステップの後に、「ストレージサブシステムの初期化の待機」タスクが失敗する可能性があります。 可能であれば、BIOS で VMD をオフにして遅延を回避します。VMD をオンにしておく必要がある場合は、初期セットアップで使用する NVMe ドライブを減らしてみてください。ドライブが多いほど初期化に時間がかかるためです。	4.3 (6.250077)	6.0(1.250162) 6.0(1.250174)

Cisco UCS X シリーズ M8、M7 6.0(1.250122)、M6、B シリーズ M6、M56.0(1.250127) および C シリーズ M8、M7、M6 6.0(1.250131)サーバファームウェアリリースの解決済みの問題

ここでは、解決済みの問題について簡単に説明します。

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwq58890	Cisco UCS VIC 15000 シリーズ アダプタのファームウェアが更新され、まれに発生する断続的なメモリの問題が修正され、さまざまなメモリタイプおよび構成でより堅牢なかつ一貫性のある動作が保証されます。 (注) それでもメモリエラーが発生する場合は、Cisco TAC にお問い合わせください。	X シリーズ : 6.0 (1.250120) B シリーズ : 6.0 (1.250126) C シリーズ : 6.0 (1.250127)	X シリーズ : 6.0(1.250122) B シリーズ : 6.0(1.250127) C シリーズ : 6.0(1.250131)

Cisco UCS C シリーズ M8、M7 および M6 6.0(1.250127)サーバファームウェア リリースで解決された不具合

ここでは、解決済みの問題について簡単に説明します。

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwn99720	2 ソケット プラットフォームのシングル CPU セットアップで構成された Intel プロセッサと R1S CPU を搭載した Cisco UCS C シリーズ M8 サーバでは、Intel SGX は BIOS で有効にした後も無効のままになります。この問題は、デュアル CPU 構成では発生しません。	4.3(6.250039)	6.0(1.250127) 4.3(6.250044)



第 6 章

未解決の問題

Cisco バグ検索ツールを使用して、未解決の問題、解決済みの問題、およびセキュリティ修正を表示できます。

- Cisco UCS X シリーズ M8、M7、M6 6.0(2.260069)、および C シリーズ M8、M7、M66.0(2.260069)、および B シリーズ M6 6.0(2.260069) サーバ ファームウェア リリースの未解決の不具合 (68 ページ)
- Cisco UCS B シリーズ M5 6.0(1.260012) サーバ ファームウェア リリースで未解決の問題：なし (68 ページ)
- Cisco UCS X シリーズ M8、M7、M6 6.0(2.260040)、XE シリーズ M8 6.0(2.260042)、C シリーズ M8、M7、M6 6.0(2.260044)、および B シリーズ M6 6.0(2.260040) サーバ ファームウェア リリースの未解決の問題 (68 ページ)
- XE シリーズ M8 サーバ ファームウェア リリース 6.0(1.260001) の未解決の問題：なし (72 ページ)
- Cisco UCS C シリーズ サーバ M8 ファームウェア リリース 6.0(1.250194) の未解決の問題：なし (72 ページ)
- X シリーズ M8 6.0(1.252114) および C シリーズ M8 6.0(1.250192) サーバ ファームウェア リリースの未解決の問題 (72 ページ)
- XE シリーズ M8 サーバ ファームウェア リリース 6.0(1.251030) の未解決の問題 (73 ページ)
- X シリーズ M8 サーバ ファームウェア リリース 6.0(1.252039) の未解決の問題：なし (76 ページ)
- Cisco UCS X シリーズ M8、M7 6.0(1.250162)、M6、B シリーズ M6、M56.0(1.250157) および C シリーズ M8、M7、M6 6.0(1.250174) サーバ ファームウェア リリースの未解決の問題：なし (76 ページ)
- Cisco UCS X シリーズ M8、M7 6.0(1.250122)、M6、B シリーズ M6、M56.0(1.250127) および C シリーズ M8、M7、M6 6.0(1.250131) サーバ ファームウェア リリースで未解決の問題：なし (76 ページ)
- Cisco UCS X シリーズ M8、M7 6.0(1.250120)、M6、B シリーズ M6、M56.0(1.250126) および C シリーズ M8、M7、M6 6.0(1.250127) サーバ ファームウェア リリースの未解決の問題 (76 ページ)

Cisco UCS X シリーズ M8、M7、M6 6.0(2.260069)、および C シリーズ M8、M7、M66.0(2.260069)、および B シリーズ M6 6.0(2.260069) サーバー ファームウェア リリースの未解決の不具合

このセクションでは、未解決の問題について簡単に説明します。

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCws49799	Cisco UCS C シリーズ サーバーでは、ESXi 9 での仮想マシン (VM) 操作中にホットプラグした後、アウトオブバンド (OOB) インターフェイスでドライブが誤って劣化として報告される場合があります。この問題は、システムが特定の NVMe-MI コマンド応答を適切に処理できず、不正確な評価指標と、物理ドライブの再装着後もクリアされない永続的な誤った正常性アラートが発生するために発生します。	この問題の直接的な回避策はありません。この問題は、システムがデバイスの応答を処理する方法を強化するコードの改善によって対処されています。	C シリーズ : 6.0 (2.260068)

Cisco UCS B シリーズ M5 6.0(1.260012) サーバ ファームウェア リリースで未解決の問題 : なし

Cisco UCS X シリーズ M8、M7、M6 6.0(2.260040)、XE シリーズ M8 6.0(2.260042)、C シリーズ M8、M7、M6 6.0(2.260044)、および B シリーズ M6 6.0(2.260040) サーバー ファームウェア リリースの未解決の問題

このセクションでは、未解決の問題について簡単に説明します。

不具合 ID	説明	回避策	影響を受ける最初のバージョン
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。	サーバーを再起動して vNIC 接続を復元します。	4.3(5.250030)
CSCwt34436	Cisco Unified Edge サーバー (UCSXE-130C-M8-20、UCSXE-130C-M8-32) では、サーバーインベントリ完了の待機 タスクでサーバー検出ワークフローが失敗します。この問題は、Unified Edge のアップグレード後に発生し、インベントリ収集 タスクでサーバー検出ワークフローが停止し、4 台のサーバーのうち 3 台に影響を及ぼします。	サーバーの検出を正常に完了するには、個々のサーバーで「再検出」を手動で開始します。	6.0(2.260042)
CSCws19521	UCSX-X10C-PT4F コントローラを搭載した Cisco UCS x210C M8 サーバの 6.0 (2.260040) より前のリリースへのサーバーファームウェアのダウングレードは、複雑なプログラマブルロジックデバイス (CPLD) のファームウェアバージョンの不一致により失敗します。	HFP から CPLD コンポーネントを除外します。	6.0(2.260040)

Cisco UCS X シリーズ M8、M7、M6 6.0(2.260040)、XE シリーズ M8 6.0(2.260042)、C シリーズ M8、M7、M6 6.0(2.260044)、および B シリーズ M6 6.0(2.260040) サーバー ファームウェア リリースの未解決の問題

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCwt42347	ホスト ファームウェア パッケージ (HFP) をリリース 4.3 (2) から 6.0 (2) にアップグレードする際、UCSX-X10C-RAIDF コントローラを搭載した Cisco UCS X シリーズ サーバでは、ハードウェア構成を確認するための準備の段階で障害が発生し、結果としてユニファイド BIOS 管理 (UBM) アップグレードがハングします。ファームウェアの更新プロセスが完了せず、BMC ログには更新プロセスが無限に実行されていることが示されます。	既知の回避策はありません。 この問題は、UBM ファームウェアの更新が必要な場合に発生します。UBM コンポーネントは、UCSX-X10C-RAIDF コントローラにのみ影響します。UBM 部品を含む他のメザニンカードには影響しません。	6.0(2.260040)

不具合 ID	説明	回避策	影響を受ける最初のバージョン
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、4.3 (6.260003)、6.0 (1.250192)、および 6.0 (2.260044) 以降です。 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。	6.0(2.260044) 6.0(1.250192) 4.3(6.260003)

不具合 ID	説明	回避策	影響を受ける最初のバージョン
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。	既知の回避策はありません。	X シリーズ : 6.0(2.260040) XE シリーズ : 6.0(2.260042) C シリーズ : 6.0(2.260044) B シリーズ : 6.0(2.260040)

XE シリーズ M8 サーバ ファームウェア リリース 6.0(1.260001) の未解決の問題 : なし

Cisco UCS C シリーズ サーバ M8 ファームウェア リリース 6.0(1.250194) の未解決の問題 : なし

X シリーズ M8 6.0(1.252114) および C シリーズ M8 6.0(1.250192) サーバ ファームウェア リリースの未解決の問題

このセクションでは、未解決の問題について簡単に説明します。

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCwr82017	Cisco UCS X210c M8、C220 M8、および C240 M8 サーバでは、Intel SGX を有効にし、システム メモリ 設定で PRMRR サイズをサポートされていない値に設定すると、システムが継続的に再起動します。サポートされていないサイズが構成された時のみにこの問題が発生します。	Intel SGX を有効にする場合は、PRMRR サイズをサポートされている値に設定してください。	X シリーズ M8 : 6.0(1.252114) C シリーズ M8 : 6.0(1.250192)

XE シリーズ M8 サーバファームウェア リリース 6.0(1.251030) の未解決の問題

このセクションでは、未解決の問題について簡単に説明します。

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCwr05911	Cisco Unified Edge サーバでは、ホストの電源がオフになると、IMM インベントリ ページには、LOM-NIC-1 インターフェイスが eCMC:A で up と表示されるが、eCMC:B で down と表示されます。この不整合は、ホストの電源がオフのときにのみ発生します。この問題による機能への影響はありません。	既知の回避策はありません。	6.0(1.251030)

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCwr63339	Cisco Unified Edge サーバでは、ランタイム時にシャーンが不十分な電源状態になった場合（ノードの BMC がすでに起動した後）、前面パネルの物理電源ボタンを使用して CPU に電力を供給できます。これにより、特定のログ/イベントで示されているように、そのノードの BMC が不安定になる可能性があります。この問題は、サーバーが起動する前にシャーンがすでに電力不足状態になっている場合は発生しません。	電力使用量が高くなっているノードを削除するか、ワット数の高い電源ユニット（PSU）にアップグレードして十分な電力を供給できます。	6.0(1.251030)
CSCwr88145	Cisco UCS XE M8 サーバでは、ポート速度が 1 Gbps に設定されている場合、ネットワークケーブルが外された後でも、2x10G 前面ポート（FP）の LED は点灯したままです。 LED は、サーバの完全な電源再投入後にのみ消灯します。	1 Gbps ポートからケーブルを外した後、サーバーを再起動して LED を消灯します。	6.0(1.251030)

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCwr04128	Cisco Unified Edge サーバーでは、Intersight ワークフローでサーバー検出が断続的に失敗し、「Adapter model CPUIntegratedNIC is not supported」というエラーメッセージが表示されます。この問題は時々発生し、すべての検出試行には影響しません。	解決するには、このエラーが表示されたときに検出プロセスを再度開始します。	6.0(1.251030)
CSCwd72323	非常にまれな内部CPUの問題が原因で、コンピューティングスレッドの電源オフに失敗する場合があります。電源オフプロセス中に、CPUはSLP4_NおよびSLP3_Nの信号を低く設定しないため、システムの電源がオフになりません。IMMを介した手動で電源操作を行うと、ホストの電源を設定できませんでした、またはタイマーが期限切れになりましたなどのエラーが返される場合があります。この問題は次のACサイクルまで維持されます。	通常の動作を復元するには、コンピューティングスレッドのACサイクルを実行します： 1. Intersight にログインします。 2. 統合 Edge > 統合 Edge シャーシへの移動 3. 右側のアクション ドロップダウンメニューを開きます 4. 電源の再投入に関するユニファイド Edge スロットをクリックし、サーバのスロット番号を入力して、電源の再投入ボタンを押します。 システムは数分後に動作可能になります。	6.0(1.251030)

X シリーズ M8 サーバファームウェア リリース 6.0(1.252039) の未解決の問題 : なし

Cisco UCS X シリーズ M8、M7 6.0(1.250162)、M6、B シリーズ M6、M5 6.0(1.250157) および C シリーズ M8、M7、M6 6.0(1.250174) サーバファームウェア リリースの未解決の問題 : なし

Cisco UCS X シリーズ M8、M7 6.0(1.250122)、M6、B シリーズ M6、M5 6.0(1.250127) および C シリーズ M8、M7、M6 6.0(1.250131) サーバファームウェア リリースで未解決の問題 : なし

Cisco UCS X シリーズ M8、M7 6.0(1.250120)、M6、B シリーズ M6、M5 6.0(1.250126) および C シリーズ M8、M7、M6 6.0(1.250127) サーバファームウェア リリースの未解決の問題

このセクションでは、未解決の問題について簡単に説明します。

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCws30219	Cisco UCS M7 サーバは、ECC（エラー訂正コード）メモリエVENTによってトリガーされたホストロックアップの影響を受けます。 これは、エラー状態時にサーバの BIOS が EFI（Extensible Firmware Interface）と通信する仕組みに特に関連しています。これらのイベント中、BIOS は必要な変数を正しく取得せず、EFI は無効なパラメータを返します。その結果、オペレーティングシステムは通常の動作を続行できず、エラーをログに記録せずにフリーズします。これが発生すると、ホストは応答しなくなり、KVM（キーボード、ビデオ、マウス）入力を受け入れられません。 シングルビット ECC エラー（DDR5 仕様によりログは記録されません）がこの状態をトリガーする可能性があり、その結果、ホストの応答性が完全に失われます。	サーババンドルをダウングレードします： • X シリーズサーバの場合は、サーババンドルをバージョン 5.4 (0.250040) またはそれ以前のリリースにダウングレードします。 • C シリーズサーバの場合は、サーババンドルをバージョン 4.3 (6.250044) またはそれ以前のリリースにダウングレードします。	X シリーズ M7:5.4 (0.250048) C シリーズ M7:4.3 (6.250053)

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCwq61388	CIMC 4.3.5 以降を実行している Cisco UCS C シリーズ M6 サーバーで、複数の NVME ドライブがある状態で BIOS の VMD を有効にすると、ストレージサブシステムの初期化が 15 分を超え、Intersight サーバー プロファイルの展開が失敗する可能性があります。VMD を無効にするか、ドライブの数を減らすと、問題を解決できます。以前のファームウェアバージョンは影響を受けません。	• VMD が必要ない場合は、VMD を無効にします。 • VMD を無効にすることが不可能な場合は、セットアップで最小数の NVME ドライブを使用します。ドライブが増えるとシステムのスタートアップが遅くなるためです。	4.3(5.250001)
CSCwm33093	マイクロチップベースのストレージカードでは、ファームウェアはパフォーマンスを最適化するためにドライブの割り当てを自動的に変更し、管理ツールからのユーザー設定を無視するので、すべてのディスクがオンラインの場合でも、仮想ドライブ (VD) は「動作不能」として表示されます。	arcconf の出力により、スパン内のドライブの割り当てを確認します。パフォーマンスを向上させるために、ファームウェアが管理ツールの設定を上書きする場合があります。	4.3(5.240134)

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCwq17020	UCSX-X10C-RAIDF コントローラ の背後に 3.8TB 以上の容量の U3 Micron ドライブを JBOD モードで取り付けした後、EFI ブートイメージのロードに関連する BIOS エラーが原因で Linux OS が起動に失敗します。 この問題は、特に Intel® プロセッサを搭載した Cisco UCS X シリーズ M8 サーバーで発生し、複数の Linux ディストリビューションに影響します。ドライブを RAID 0 で構成した場合、この問題は発生しません。 Microsoft Windows® および Linux OS は、より小容量のドライブを使用した場合や RAID 0 を使用した場合、正常に起動します。	RAIDで構成されたドライブにOSをインストールします。	X210c:5.4 (0.250037) X215c:5.4 (0.250035)

Cisco UCS X シリーズ M8、M7 6.0(1.250120)、M6、B シリーズ M6、M56.0(1.250126) および C シリーズ M8、M7、M6 6.0(1.250127) サーバファームウェア リリースの未解決の問題



第 7 章

既知の問題

このリリースで未解決のバグおよび解決済みのバグには、[Cisco バグ検索ツール](#) を使用してアクセスできます。



(注) Cisco Bug Search Tool にログインしてこのツールを使用するには、[Cisco.com](#) アカウントが必要です。アカウントがない場合は、[アカウントを登録](#)できます。

Cisco Bug Search Tool の詳細については、[Bug Search Tool \(BST\) ヘルプ](#)および[FAQ](#)を参照してください。

- [Cisco UCS B シリーズ M5 6.0\(1.260012\) サーバファームウェア リリースで既知の問題：なし \(82 ページ\)](#)
- [Cisco UCS X シリーズ M8、M7、M6 6.0\(2.260040\)、XE シリーズ M8 6.0\(2.260042\)、C シリーズ M8、M7、M6 6.0\(2.260044\)、および B シリーズ M6 6.0\(2.260040\) サーバファームウェア リリースの既知の問題 \(82 ページ\)](#)
- [XE シリーズ M8 サーバファームウェア リリース 6.0\(1.260001\) の既知の問題：なし \(84 ページ\)](#)
- [Cisco UCS C シリーズ サーバ M8 ファームウェア リリース 6.0\(1.250194\) の既知の問題：なし \(84 ページ\)](#)
- [Cisco UCS X シリーズ M8 6.0\(1.252114\)、M7、M6 6.0\(1.250179\)、B シリーズ M6、M5 6.0\(1.250169\)、および C シリーズ M8、M7、M6 6.0\(1.250192\) サーバファームウェア リリースで既知の問題：なし \(84 ページ\)](#)
- [XE シリーズ M8 サーバファームウェア リリース 6.0\(1.251030\) の既知の問題 \(84 ページ\)](#)
- [Cisco UCS X シリーズ M8、M7 6.0\(1.250162\)、M6、B シリーズ M6、M5 6.0\(1.250157\) および C シリーズ M8、M7、M6 6.0\(1.250174\) サーバファームウェア リリースで既知の問題：なし \(85 ページ\)](#)
- [Cisco UCS X シリーズ M8、M7、M6 6.0\(1.250122\)、B シリーズ M6、M5 6.0\(1.250127\) および C シリーズ M8、M7、M6 6.0\(1.250131\) サーバファームウェア リリースの既知の問題：なし \(85 ページ\)](#)
- [Cisco UCS C シリーズ M8、M7 および M6 6.0\(1.250127\) サーバファームウェア リリースの既知の問題 \(86 ページ\)](#)

Cisco UCS B シリーズ M5 6.0(1.260012) サーバファームウェアリリースで既知の問題：なし

Cisco UCS X シリーズ M8、M7、M6 6.0(2.260040)、XE シリーズ M8 6.0(2.260042)、C シリーズ M8、M7、M6 6.0(2.260044)、および B シリーズ M6 6.0(2.260040) サーバファームウェアリリースの既知の問題

ここでは、解決済みの問題について簡単に説明します。

不具合 ID	説明	影響を受ける最初のバージョン	リリースで解決済み
CSCwr72707	2 台以上の Kioxia E3.S CD8P 1.9 T NVMe ドライブを搭載した Cisco UCS C220 M8、C240 M8 では、同時テスト中にランダム 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、ドライブあたり 1,600kIOPS の定格からドライブあたり約 680k の入出力処理数/秒 (IOPS) に低下する可能性があります。単一ドライブのテストは期待されるパフォーマンスを満たし、問題は複数ドライブのセットアップでのみ発生することを示しています	このパフォーマンスのボトルネックを解決するには、Red Hat Enterprise Linux (RHEL) のブート設定で、次の Intel が推奨するカーネルチューニング 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： <pre>intel_pstate=disable pci=pcie_bus_safe</pre> • 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： <pre>intel_pstate=disable pci=pcie_bus_safe nvme.poll_queues=32 intel_iommu=on</pre>	X シリーズ：6.0(2.260040) XE シリーズ：6.0(2.260042) C シリーズ：6.0(2.260044) B シリーズ：6.0(2.260040)

XE シリーズ M8 サーバ ファームウェア リリース 6.0(1.260001) の既知の問題：なし

Cisco UCS C シリーズ サーバ M8 ファームウェア リリース 6.0(1.250194) の既知の問題：なし

Cisco UCS X シリーズ M8 6.0(1.252114)、M7、M6 6.0(1.250179)、B シリーズ M6、M5 6.0(1.250169)、および C シリーズ M8、M7、M6 6.0(1.250192) サーバ ファームウェア リリースで既知の問題：なし

XE シリーズ M8 サーバ ファームウェア リリース 6.0(1.251030) の既知の問題

このセクションでは、既知の問題について簡単に説明します。

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCws25068	Unified Edge サーバーにカーネルバージョン 6.8.0-71 の Ubuntu 24.04.3 をインストールすると、統合ネットワークカード (ICE ドライバ) が検出されず、ネットワーク設定と接続が妨げられます。この問題は、カーネル 6.8.0-71 がこのプラットフォームの NIC の ICE ドライバをサポートしていないために発生します。	1. Ubuntu Node リリース ページ から GA ISO をダウンロードし、ブート可能 USB またはリモート対応メディアを使用してインストールします。 2. Ubuntu Security Pool から必要な 6.8.0-80 カーネル パッケージ (.deb ファイル) をダウンロードします。 3. すべての .deb ファイル (linux-image、linux-headers、linux-modules、linux-modules-Extra、linux-tools) をフォルダに配置し、genisoimage や mkisofs などのツールを使用して ISO を作成します。 4. Ubuntu のインストール後に、サーバーに ISO をマウントします。 5. dpkg -i X.deb を使用してカーネル パッケージをインストールします。 6. サーバーを再起動し、カーネルバージョンが 6.8.0 ~ 80 であることを確認します。 統合ネットワークカードが検出され、設定に使用できるようになります。	6.0(1.251030)

Cisco UCS X シリーズ M8、M7 6.0(1.250162)、M6、B シリーズ M6、M56.0(1.250157) および C シリーズ M8、M7、M6 6.0(1.250174) サーバーファームウェアリリースで既知の問題：なし

Cisco UCS X シリーズ M8、M7、M6 6.0(1.250122)、B シリーズ M6、M56.0(1.250127) および C シリーズ M8、M7、M6

6.0(1.250131)サーバファームウェアリリースの既知の問題：なし

Cisco UCS C シリーズ M8、M7 および M6 6.0(1.250127)サーバファームウェアリリースの既知の問題

このセクションでは、既知の問題について簡単に説明します。

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCwn95239	Cisco UCS サーバでは、BIOS の破損が原因でサーバの電源がオンになりません。次のメッセージが表示されます。「電源投入失敗がアサート済み（電源投入失敗、サーバの電源投入失敗）」 この問題は、次のシナリオで特に BIOS の更新操作が中断された場合に発生する可能性があります： • BIOS フラッシュまたは更新の中断（例：更新中の強制的な電源の再投入）。 • BIOS 更新中の CMOS クリア操作の開始。 • BIOS 更新中の工場出荷時デフォルトへの復元。 • BIOS 更新中の Cisco IMC のリブート。 • BIOS の更新プロセスを中断させるその他の予期しない操作の実行。	次のいずれかを実行します。 • CIMC をリブートします。同様に、BIOS のアクティブ化であるリカバリメカニズムが開始されます。 • バックアップ BIOS の Activate。 • BIOS を更新し、アクティブ化します。	4.3(6.250039)

不具合 ID	説明	回避策	影響を受ける最初のバージョン
CSCwe68248	HUU 4.3(3.240xxx) レベルのファームウェアを実行し、2つの PCIe VIC と 1 つの MLOM VIC を持つ Cisco UCS C220M7 および C240 M7 サーバで、サーバファームウェアを HUU 4.3(4.xxxxxx) または 4.3(5.xxxxxx) または 4.3(Redfish API インターフェイスを使用して 6.xxxxx) 以降のレベルで実行した場合、UCSUpdate タスクは CiscoCard モードが設定されている PCIe VIC (riser1) の誤った更新失敗を報告します。ただし、ファームウェアはバックグラウンドで正常に更新およびアクティブ化されます。 (注) 言及されている HUU バージョン番号の「xxxx」は、シリーズ内で利用可能なすべてのバージョンを表します。	回避策はありません。誤った障害の更新を無視します。	4.3(3.240043)



第 8 章

互換性

- [バージョンをまたがるファームウェアのサポート](#) (89 ページ)

バージョンをまたがるファームウェアのサポート

XE シリーズ サーバー ファームウェア バージョン	eCMC インフラストラクチャ ファームウェア バージョン	
	6.0(1)	6.0(2)
6.0(2)	○	○
6.0(1)	○	○

X シリーズ サーバー ファームウェア バージョン	インフラストラクチャ ファームウェア バージョン										
	4.1(3)	4.2(1)	4.2(2)	4.2(3)	4.3(2)	4.3(3)	4.3(4)	4.3(5)	4.3(6)	6.0(1)	6.0(2)
6.0(2)	N/A	非対応	非対応	○	○	○	○	○	○	○	○
6.0(1)	N/A	非対応	非対応	○	○	○	○	○	○	○	○
5.4(0)	N/A	非対応	非対応	○	○	○	○	○	○	○	○

5.3(0)	N/A	非対応	非対応	○	○	○	○	○	○	○	○
5.2(2)	N/A	非対応	非対応	○	○	○	○	○	○	○	○
5.2(1)	N/A	非対応	非対応	○	○	○	○	○	○	○	○
5.2(0)	N/A	非対応	非対応	○	○	○	○	○	○	○	○
5.1(1)	N/A	非対応	非対応	○	○	○	○	○	○	○	○
5.1(0)	N/A	非対応	非対応	○	○	○	○	○	○	○	○
5.0(4)	N/A	○	○	○	○	○	○	○	○	○	○
5.0(2)	N/A	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応	非対応
5.0(1)	N/A	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応	非対応

C シリーズ サーバ ファーム ウェア バージョン	インフラストラクチャ ファームウェア バージョン										
	4.1(3)	4.2(1)	4.2(2)	4.2(3)	4.3(2)	4.3(3)	4.3(4)	4.3(5)	4.3(6)	6.0(1)	6.0(2)
6.0(2)	非対応	非対応	非対応	○	○	○	○	○	○	○	○
6.0(1)	非対応	非対応	非対応	○	○	○	○	○	○	○	○
4.3(6)	○	○	○	○	○	○	○	○	○	○	○
4.3(5)	○	○	○	○	○	○	○	○	○	○	○

4.3(4)	○	○	○	○	○	○	○	○	○	○	○
4.3(3)	○	○	○	○	○	○	○	○	○	○	○
4.3(2)	○	○	○	○	○	○	○	○	○	○	○
4.3(1)	○	○	○	○	○	○	○	○	○	○	○
4.2(3)	○	○	○	○	○	○	○	○	○	○	○
4.2(2)	○	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応	非対応
4.2(1)	○	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応	非対応
4.1(3)	○	○	○	○	非対応	非対応	非対応	非対応	非対応	非対応	非対応

B シリーズサーバファームウェアバージョン	インフラストラクチャ ファームウェア バージョン										
	4.1(3)	4.2(1)	4.2(2)	4.2(3)	4.3(2)	4.3(3)	4.3(4)	4.3(5)	4.3(6)	6.0(1)	6.0(2)
6.0(2)	非対応	非対応	非対応	○	○	○	○	○	○	○	○
6.0(1)	非対応	非対応	非対応	○	○	○	○	○	○	○	○
5.4(0)	○	○	○	○	○	○	○	○	○	○	○
5.3(0)	○	○	○	○	○	○	○	○	○	○	○
5.2(2)	○	○	○	○	○	○	○	○	○	○	○
5.2(1)	○	○	○	○	○	○	○	○	○	○	○
5.2(0)	○	○	○	○	○	○	○	○	○	○	○
5.1(0)	○	○	○	○	○	○	○	○	○	○	○

4.3(3)	○	○	○	○	○	○	○	○	○	○	○
4.3(2)	○	○	○	○	○	○	○	○	○	○	○
4.2(3)	○	○	○	○	○	○	○	○	○	○	○
4.2(2)	○	○	○	○	非対 応	非対 応	非対 応	非対 応	非対 応	非対 応	非対 応
4.2(1)	○	○	○	○	非対 応	非対 応	非対 応	非対 応	非対 応	非対 応	非対 応
4.1(3)	○	○	○	○	非対 応	非対 応	非対 応	非対 応	非対 応	非対 応	非対 応



第 9 章

関連資料

- [関連資料 \(93 ページ\)](#)

関連資料

- [Cisco Intersight のリリース ノートとリリース バンドル](#)
- [Cisco UCS C885A M8 ラック サーバーの Cisco Baseboard Management Controller リリース ノート](#)
- [『Release Notes for Cisco UCS Manager』](#)
- [Cisco UCS ラック サーバー ソフトウェアのリリース ノート](#)
- [Cisco UCS Manager と Intersight のリリース戦略](#)
- 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 Intersight Unified Edge eCMC Infrastructure Firmware Release、6.0 のリリース ノート](#)
- [Unified Edgeのリリース ノートとリリース バンドル](#)
- [Unified Edgeでのファームウェアの管理](#)

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。