Cisco Intersight 管理モードサーバファームウェア、リリース 4.3、5.2、5.3 および 5.4

© 2025 Cisco and/or its affiliates. All rights reserved.

目次

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Intersight 管理モードサーバファームウェア、リリース 4.3、5.2、5.3 および 5.4

Cisco Intersight は、物理および仮想インフラストラクチャの合理的な展開、モニタリング、管理、サポートのための機能を有効にします。Cisco Unified Computing System（UCS）サーバとサードパーティのデバイスをサポートし、高度な管理およびサポート機能を提供するとともに、インフラストラクチャの正常性とステータスをグローバルに可視化します。

主な機能：

- 問題発生時に手動操作なしでテレメトリデータを分析できます。
- サービスリクエスト（SR）と返品許可（RMA）の処理を自動的に開始します。

Cisco Intersight は、次の Cisco UCS サーバを管理します。

- Intersight 管理対象モード（IMM）B シリーズ、C シリーズ、および X シリーズサーバー（FI 接続）
- C シリーズスタンドアロンサーバー
- スタンドアロンモードの Cisco UCS 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。
- UCSM 管理対象モード（UMM）B シリーズ、C シリーズサーバー、および X シリーズサーバー（FI 接続）
- UCSM 管理モード（UMM）の Cisco UCS 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。

このドキュメントでは、Cisco Intersight 管理モード（IMM）に焦点を当てた情報を提供します。内容は次のとおりです。

- アダプタ、BIOS、CIMC、RAID コントローラ、ディスクファームウェアなど、コンピューティングノードコンポーネントに関する新機能、解決済みの問題、未解決の問題、および回避策に関する情報。
- 初版発行後のアップデート。
- このリリースに関連付けられているブレード、ラック、モジュラサーバやその他の Cisco Unified Computing System（UCS）コンポーネントに関連するファームウェアおよび BIOS

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。

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 4.3(6)

© 2025 Cisco and/or its affiliates. All rights reserved.

改訂日	説明
2025 年 5 月 22 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 X210C M8 サーバファームウェアリリース 5.4（0.250044） • Cisco UCS X215C M8、X410C M7、および X210C M7 サーバファームウェアリリース 5.4（0.250040） • Cisco UCS C シリーズ M8 および M7 サーバファームウェア、リリース 4.3(6.250044) 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 および M7 サーバファームウェアリリース 4.3（6.250044）で解決された問題 新しいハードウェアのサポート、セキュリティ修正、未解決の問題は含まれていません。
2025 年 4 月 30 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 X210c M8 サーバファームウェアリリース 5.4（0.250037） • Cisco UCS X215c M8、X210c M7、および X410c M7 サーバファームウェアリリース 5.4（0.250035） • Cisco UCS X210c M6 サーバファームウェアリリース 5.4（0.250033） • Cisco UCS C シリーズ M7 および M6 サーバファームウェア、リリース 4.3（6.250040） • Cisco UCS C225 M8 および C245 M8 サーバファームウェアリリース 4.3（6.250040） • Cisco UCS C220 M8 および C240 M8 サーバファームウェアリリース 4.3（6.250039） • 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 5.4（0.250034） 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 X シリーズ M8 5.4(0.250037) および C シリーズ M8 サーバ 4.3(6.250039) ファームウェアリリース • クロスバージョンファームウェアサポート • B シリーズ M5 5.4(0.250034) サーバファームウェアリリース のセキュリティ修正 • C シリーズ M8 ファームウェアリリース 4.3(6.250040) および 4.3(6.250039) で解決された問題 • X シリーズ M8 5.4（0.250037）および 5.4（0.250035）、M7 5.4（0.250035）、M6 5.4（0.250033）、および B シリーズ M6、M5 5.4（0.250034）サーバファームウェアリリースで解決された問題 • X シリーズ M8 5.4（0.250037）および C シリーズ M8 4.3（6.250040）および 4.3（6.250039）、M7、M6 4.3（6.250040）サーバファームウェアリリースの未解決の問題 • 既知の動作と制限事項

表 2 リリース 4.3(5)

© 2025 Cisco and/or its affiliates. All rights reserved.

改訂日	説明
2025 年 5 月 19 日	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 4.3(5.250033) のリリースノートを更新しました。 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 および M6 サーバファームウェアリリース 4.3(5.250033) で解決された不具合 新しいハードウェアのサポート、セキュリティ修正、未解決の問題は含まれていません。
2025 年 4 月 10 日	Cisco UCS X シリーズ Direct FI インフラストラクチャファームウェアバージョン 4.3（5.250033）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。
2025 年 3 月 25 日	Cisco UCS C シリーズ M7 および M6 サーバファームウェアリリース 4.3(5.250033) のリリースノートを更新しました 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 M7 および M6 サーバファームウェアリリース 4.3(5.250030) のセキュリティ修正 • 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 4.3(5.250030) で解決された不具合 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。
2025 年 3 月 5 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 サーバファームウェアリリース 5.3(0.250021) • 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 5.3(0.250021) このリリースには、X シリーズ M8、M7、M6 5.3（0.250021）および B シリーズ M6、M5 5.3（0.250021）サーバファームウェアリリースで解決された問題に対する更新が含まれています。 新しいハードウェアのサポート、セキュリティ修正、未解決の問題は含まれていません。
2025 年 1 月 20 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 サーバファームウェアリリース 5.3(0.250001) • 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 5.3(0.250001) • 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 4.3(5.250001) このリリースには、以下への更新が含まれます。 • X シリーズ M8 5.3(0.250001) および C シリーズ M8 4.3(5.250001) サーバファームウェアリリースの新しいハードウェア • X シリーズ M8、M7、M6 5.3(0.250001) および B シリーズ M6、M5 5.3(0.250001)サーバファームウェアリリースで解決された不具合 • C シリーズ M8、M7 および M6 4.3(5.250001)サーバファームウェアリリースで解決された問題 セキュリティ修正や未解決の問題は含まれていません。

© 2025 Cisco and/or its affiliates. All rights reserved.

改訂日	説明
2024 年 11 月 15 日	X シリーズファームウェアリリース 5.3（0.240016）で解決された問題に CSCwm06766 を追加しました。
2024 年 10 月 22 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 サーバファームウェアリリース 5.3(0.240016) • 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 5.3(0.240014) • 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 4.3(5.240021) このリリースには、以下への更新が含まれます。 • X シリーズおよび C シリーズ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 • クロスバージョンファームウェアサポート • X シリーズ 5.3(0.240016) および B シリーズ 5.3(0.240014) サーバファームウェアリリースのセキュリティ修正 • X シリーズファームウェアリリース 5.3(0.240016) で解決された不具合 • C シリーズサーバファームウェアリリース 4.3(5.240021) で解決された不具合 • C シリーズサーバファームウェアリリース 4.3（5.240021）で未解決の問題 • X シリーズサーバファームウェアリリース 5.3（0.240016）で未解決の問題

表 3　　リリース 4.3(4

改訂日	説明
2024 年 12 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 M7 5.2(2.240080)および M6 5.2(2.240078) サーバファームウェアリリース • 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 5.2(2.240080) • Cisco UCS C シリーズ M7 および M6 サーバファームウェア、リリース 4.3(4.242066) このリリースには、以下への更新が含まれます。 • X シリーズ M7 5.2(2.240080) および M6 5.2(2.240078) サーバファームウェアリリースで解決された問題 • B シリーズ M6 および M5 サーバファームウェアリリース 5.2(2.240080) で解決された不具合 • C シリーズ M7 および M6 サーバファームウェアリリース 4.3(4.242066) で解決された不具合 新しいハードウェアのサポート、セキュリティ修正、未解決の問題は含まれていません。

© 2025 Cisco and/or its affiliates. All rights reserved.

改訂日	説明
2024 年 11 月 15 日	X シリーズ M7 5.2（2.240074）、X シリーズ M6 5.2（2.240073）、および B シリーズ M6 5.2（2.240073）ファームウェアリリースのセキュリティ修正の元で追加された CSCwk62723。
2024 年 10 月 10 日	以下の各セクションが更新されました。 • X シリーズ M7 サーバファームウェアリリース 5.2(2.240074) による解決済みの問題 • C シリーズ M6 サーバファームウェアリリース 4.3(4.242038) で解決済みの問題
2024 年 10 月 3 日	C シリーズ M7 サーバファームウェアリリース 4.3(4.242038) の新しいハードウェア機能の更新
2024 年 9 月 26 日	Cisco UCS C シリーズ M7 および M6 サーバファームウェア、リリース 4.3(4.242038) のリリースノートを更新しました。 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 M6 サーバファームウェアリリース 4.3(4.242038) のセキュリティ修正 • C シリーズ M6 サーバファームウェアリリース 4.3(4.241063) で解決された不具合 • C シリーズ M6 ファームウェアリリース 4.3（4.242038）の未解決の問題 新しいハードウェアのサポートは含まれていません。
2024 年 9 月 3 日	Intersight インフラストラクチャファームウェアバージョン 4.3(4.240074) がリリースされました。 Cisco UCS X シリーズ M7 5.2(2.240074)、X シリーズ M6 5.2(2.240073) 、および B シリーズ M6 5.2(2.240073)サーバのファームウェアバージョンがリリースされました。新しいハードウェアのサポート、セキュリティ修正、未解決の問題、解決済みの問題は含まれていません。
2024 年 8 月 20 日	Cisco UCS C シリーズ M7 および M6 サーバファームウェア、リリース 4.3(4.241063) のリリースノートを更新しました。 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 M7 および M6 ファームウェアリリース 4.3(4.241063) で解決された不具合 • C シリーズ M7 および M6 サーバファームウェアリリース 4.3(4.241063) のセキュリティ修正 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。
2024 年 7 月 25 日	Intersight インフラストラクチャファームウェアバージョン 4.3(4.240078)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。

© 2025 Cisco and/or its affiliates. All rights reserved.

改訂日	説明
2024 年 6 月 25 日	Cisco UCS C シリーズ M8 サーバファームウェア、リリース 4.3(4.241014) のリリースノートを更新しました。 このリリースには、C シリーズ M8 サーバファームウェアリリース 4.3(4.241014) の新しいハードウェア機能が含まれます。
2024 年 6 月 13 日	X シリーズ M6 および M7 ファームウェアリリース 5.2(2.240053) の解決済みの不具合が更新されました。
2024 年 6 月 5 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 X シリーズ M7 および M6 サーバファームウェア、リリース 5.2(2.240053) • 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 5.2(2.240051) • Cisco UCS C シリーズ M7、M6、および M5 サーバファームウェア、リリース 4.3(4.240152) 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 M6 および M7 サーバファームウェアリリースの新しいハードウェア機能 • B シリーズ M6 サーバおよび X シリーズ M7 および M6 サーバの新しいハードウェア機能、X シリーズ M7 および M6 サーバの未解決の問題、および X シリーズ M7 および M6 サーバの解決済みの問題。 • X シリーズ M7 および M6 サーバでの未解決の問題 • X シリーズ M7 および M6 サーバで解決された問題。

表 4 リリース 4.3(3)

改訂日	説明
2024 年 4 月 24 日	Cisco UCS C シリーズ M7 および M6 サーバファームウェア、リリース 4.3(3.240043) のリリースノートを更新しました。
2024 年 2 月 5 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 サーバファームウェア、リリース 5.2(1.240010) • Cisco UCS X シリーズ M6 サーバファームウェア、リリース 5.2(1.240010) • Cisco UCS B シリーズ M6 サーバファームウェア、リリース 5.2(1.240010) • Cisco UCS C シリーズ M7 および M6 サーバファームウェア、リリース 4.3(3.240022)

表 5 リリース 4.3(2)

© 2025 Cisco and/or its affiliates. All rights reserved.

改訂日	説明
2025 年 4 月 17 日	C シリーズファームウェアリリース 4.3（2.230270）で解決された問題に CSCwh81377 を追加。
2025 年 3 月 18 日	Cisco UCS C シリーズ M5 サーバファームウェア、リリース 4.3(2.250021) のリリースノートを更新しました。 このリリースには、C シリーズ M5 サーバファームウェアリリース 4.3（2.250021）で解決された問題に対する更新が含まれています。 新しいハードウェアのサポート、セキュリティ修正、未解決の問題は含まれていません。
2025 年 3 月 11 日	C シリーズ M5 サーバファームウェアリリース 4.3(2.250016) での未解決の問題に CSCwn97854 を追加。
2025 年 2 月 28 日	Cisco UCS C シリーズ M5 サーバファームウェア、リリース 4.3(2.250016) のリリースノートを更新しました。 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 M5 サーバファームウェアリリース 4.3(2.250016) のセキュリティ修正 • C シリーズ M5 サーバファームウェアリリース 4.3(2.250016) による解決済みの問題 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。
2024 年 12 月 9 日	Cisco UCS C シリーズ M5 サーバファームウェア、リリース 4.3(2.240107) のリリースノートを更新しました。 このリリースには、C シリーズ M5 サーバファームウェアリリース 4.3（2.240107）で解決された問題に対する更新が含まれています。 新しいハードウェアのサポート、セキュリティ修正、未解決の問題は含まれていません。
2024 年 10 月 8 日	Cisco UCS C シリーズ M5 サーバファームウェア、リリース 4.3(2.240090) のリリースノートを更新しました。 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 M5 サーバーファームウェアリリース 4.3(2.240090) のセキュリティ修正 • C シリーズ M5 サーバファームウェアリリース 4.3(2.240090) による解決済みの問題 • C シリーズ M5 サーバファームウェアリリース 4.3(2.240090) の未解決の問題 新しいハードウェアのサポートは含まれていません。
2024 年 8 月 13 日	C シリーズ M5 サーバファームウェア、リリース 4.3(2.240077) がリリースになりました。 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 M5 ファームウェアリリース 4.3(2.240077) のセキュリティ修正 • C シリーズ M5 ファームウェアリリース 4.3(2.240077) の解決済みの問題 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。

© 2025 Cisco and/or its affiliates. All rights reserved.

改訂日	説明
2024 年 6 月 3 日	C シリーズサーバファームウェアバージョン 4.3(2.240053) がリリースされました。このリリースには、セキュリティ修正と解決済みの問題の更新が含まれています。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。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。
2024 年 3 月 22 日	C シリーズサーバファームウェアバージョン 4.3(2.240037) がリリースされました。このリリースには、Cisco UCS C225 M6 および C245 M6 サーバのベースボード管理コントローラ（BMC）の機能拡張が含まれています。新しいハードウェアのサポート、セキュリティ修正、未解決の問題、解決済みの問題は含まれていません。
2024 年 4 月 17 日	「UCSM と IMM のファームウェアバージョンの同等性」の表を更新して、UCS X シリーズサーババージョン 5.1(1) を追加しました。 次の 4.3.1 リリース固有のセクションを 、*Cisco Intersight サーバファームウェア 4.2、5.0、および 5.1 のリリースノート*から Cisco Intersight サーバファームウェア 4.3 および 5.2 のリリースノート（本ドキュメント）に移動しました 。 • C シリーズファームウェア 4.3（1.230097）の新規ハードウェアサポート • C シリーズ M7 ファームウェアリリース 4.3（1.230138）で解決された問題 • C シリーズ M7 ファームウェアリリース 4.3（1.230124）で解決された問題 これは、4.3 リリース情報を統合するためのものです。
2024 年 3 月 7 日	Cisco UCS C シリーズ M7、M6、および M5 サーバファームウェア、リリース 4.3(2.240009) のリリースノートを更新しました。
2024 年 1 月 24 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 X シリーズ M7 サーバファームウェア、リリース 5.2(0.230127) • Cisco UCS X シリーズ M6 サーバファームウェア、リリース 5.2(0.230127) • Cisco UCS C シリーズ M5、M6、および M7 サーバファームウェア、リリース 4.3(2.240002) • Cisco UCS B シリーズ M5 および M6 サーバファームウェア、リリース 5.2(0.230127)
2023 年 11 月 14 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 X シリーズ M7 サーバファームウェア、リリース 5.2(0.230092) • Cisco UCS X シリーズ M6 サーバファームウェア、リリース 5.2(0.230092 • Cisco UCS C シリーズサーバファームウェアリリース 4.3(2.230270) • Cisco UCS B シリーズサーバファームウェア、リリース 5.2(0.230100)
2023 年 9 月 12 日	Cisco UCS X シリーズ 410c M7 サーバファームウェア、リリース 5.2(0.230061) のリリースノートを更新しました。

© 2025 Cisco and/or its affiliates. All rights reserved.

改訂日	説明
2023 年 8 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作成しました。 • Cisco UCS X シリーズ M7 サーバファームウェア、リリース 5.2(0.230041) • Cisco UCS X シリーズ M6 サーバファームウェア、リリース 5.2(0.230040) • Cisco UCS C シリーズサーバファームウェア、リリース 4.3(2.230207) • Cisco UCS B シリーズサーバファームウェア、リリース 5.2(0.230039)

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。

新しいハードウェア機能

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。

X シリーズ M8 5.4(0.250040)、5.4(0.250044) および M7 5.4(0.250040) 、および C シリーズ 4.3(6.250044) 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

C シリーズ M7 および M6 サーバファームウェアリリース 4.3(5.250033) の新しいハードウェア：なし

X シリーズ M8 5.4(0.250037) および C シリーズ M8 サーバ 4.3(6.250039) ファームウェアリリース

X シリーズ M8 サーバファームウェアリリース 5.4(0.250037) の新しいハードウェア

Cisco UCS X210c M8 コンピューティングノード

Cisco UCS X210c M8 コンピューティングノードは、Cisco UCS X シリーズモジュラシステムに統合された第 3 世代コンピューティングノードです。これは、データセンターとリモートサイトの環境でパフォーマンス・柔軟性向上、最適化を実現します。このエンタープライズクラスのサーバーは、ワークロード処理サービスに関して妥協することなく、市場で最高レベルの性能、汎用性、密度を実現します。7 ラックユニット（7RU）Cisco UCS X9508 シャーシには、業界 1 といえる、最大 8 個のコンピューティングノードの配置、ラックユニットあたりのコンピューティング,I/O,およびストレージの密度。

Cisco UCS X210c 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：最大 2 基の Intel ® Xeon® 6 スケーラブルプロセッサ（プロセッサあたり最大 86 コア、CPU あたり最大 336 MB レベル 3 キャッシュ）
- メモリ：32 x 256GB DDR5-4800 DIMM で最大 8TB（Intel® Xeon® 6 スケーラブルプロセッサ）
- ストレージ：
  - Cisco UCS X210c M8 に搭載された新しいパススルーフロントメザニンコントローラオプションを備えた最大 9 つのホットプラグ可能な EDSFF E3.S NVMe ドライブ

© 2025 Cisco and/or its affiliates. All rights reserved.

- 最大 6 台のホットプラグ可能なソリッドステートドライブ（SSD）、または不揮発性メモリエクスプレス（NVMe）2.5 インチドライブで、エンタープライズクラスの Redundant Array of Independent Disk（RAID）、または各レーンの PCIe Gen 5 接続を選択可能。
- 最大 2 台の M.2 SATA ドライブまたは 2 台の M.2 NVMe ドライブにより、柔軟なブートとローカルストレージを実現。機能

- オプションの前面メザニン GPU モジュール：Cisco UCS 前面メザニン GPU モジュールは、最大 2 つの U.2 または U.3 NVMe ドライブと 2 つの HHHL GPU をサポートするパッシブ PCIe Gen 4 前面メザニンオプションです。
- mLOM 仮想インターフェイスカード：
  - Cisco UCS VIC（仮想インターフェイスカード）15420 は、サーバのモジュラ型 LAN on motherboard（mLOM）スロットを占有でき、サーバあたり 50 Gbps（2x 25Gbps）の統合ファブリック接続を可能にし、セキュアブートテクノロジーによりサーバあたり 100 Gbps の接続を実現します。
  - Cisco UCS VIC 15230 は、サーバーのモジュール型 LAN on Motherboard（mLOM）スロットを占有でき、サーバあたり 100 Gbps 接続に対してセキュアなブートテクノロジーにより各シャーシのインテリジェントファブリックモジュール（IFM）に最大 100 Gbps で接続できます。
- オプションのメザニンカード：
  - 第 5 世代仮想インターフェイスカード（VIC）である Cisco UCS VIC 15422 は、シャーシの下部にあるサーバーのメザニンスロットに装着できます。このカードの I/O コネクタは、Cisco UCS X ファブリックテクノロジーにリンクします。付属のブリッジカードは、IFM コネクタを介してこの VIC の 4x 25 Gbps のネットワーク接続を拡張し、合計帯域幅をファブリックあたり 100 Gbps（サーバあたり合計 200 Gbps）にします。
  - Cisco UCS X-Fabric の Cisco UCS PCI メザニンカードは、シャーシの下部にあるサーバーのメザニンスロットに装着できます。このカードの I/O コネクタは Cisco UCS X ファブリックモジュールにリンクし、Cisco UCS X シリーズ PCIe ノードへの接続を可能にします。
  - すべての VIC メザニンカードは、Cisco X210c コンピューティングノードから Cisco UCS X シリーズ PCIe ノードへの I/O 接続も提供します。
- セキュリティ：サーバーは、オプションのトラステッドプラットフォームモジュール（TPM）をサポートします。追加機能には、セキュアブート FPGA および ACT2 偽造防止条項が含まれます。

注:

Cisco UCS X210c M8 コンピューティングノードには、次の Cisco Intersight インフラストラクチャファームウェアバージョンのいずれかが必要です。

- Cisco UCS 6400 および 6500 シリーズ FI - 4.3(6.250048) 以降。
- Cisco UCS X シリーズダイレクト FI：4.3(6.250094) 以降。

Cisco UCS X210c M8 コンピューティングノードでサポートされている周辺機器の詳細なリストについては、Cisco UCS X210c 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。

C シリーズ M8 サーバファームウェアリリース 4.3(6.250039) の新しいハードウェア機能

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco UCS C220 M8 サーバ

1RU、2 ソケットの Cisco UCS C220 M8 ラックサーバーは、高密度ラックマウントサーバーの導入を選択するお客様のニーズを満たすように設計されています。このサーバーは最新の Intel® プロセッサを組み合わせており、仮想化、コラボレーション、ベアメタルアプリケーションなど、多様なワークロードでトップレベルのパフォーマンスと効率性を実現する汎用アプリケーションおよびインフラストラクチャサーバーです。

Cisco UCS C220 M8 サーバは、Intel Xeon® 6 CPU を組み込んで Cisco UCS ラックサーバポートフォリオの機能を拡張します。セキュリティ、パフォーマンス、効率を向上させ、Intel Trust Domain Extensions（TDX）、Intel Data Streaming Accelerator（DSA）、Intel QuickAssist Technology（QAT）、Intel Advanced Matrix Extensions（AMX）、および Intel In-Memory Analytics Accelerator（IAA）などの組み込みアクセラレータによりサステナビリティの目標を達成を支援します。

従来のサーバーを最新世代の Cisco UCS C220 M8 ラックサーバーに移行・統合することで、電力と冷却、管理、メンテナンスといったサーバーの運用コスト（OpEx）を削減できます。

Cisco UCS C220 M8 サーバは、高密度でフォールトトレラントなサーバであり、商用と企業の両方の顧客に価値、パフォーマンス、柔軟性を提供します。

Cisco UCS C220 M8 サーバは、次の機能を提供します。

- CPU：最大 2 個の Intel Xeon 6700P または 6500P プロセッサ（1 または 2）
- メモリ：
  - 32 個の DIMM スロット（CPU あたり 16 DIMM）：最大 4 TB のメモリに対して最大 6400 MHz で 16、32、48、64、96、128GB DDR5
  - 32, 64GB MRDIMM、最大 8000 MT/s。
- PCI 拡張：PCIe 5.0 ハーフハイトスロットを最大 3 個または PCIe 5.0 フルハイトスロットを最大 2 個、専用 24 Gbps RAID コントローラスロット 1 個、専用 mLOM/OCP 3.0 スロット 1 個。
- RAID コントローラ：
  - SAS 4 または NVMe ハードウェア RAID をサポートする Cisco® 24 Gbps モジュラトライモード RAID コントローラ
  - Cisco 24 Gbps モジュール型トライモード SAS ホストバスアダプタ（HBA）
- 内蔵ストレージ：

  バックプレーンオプション：
  - 最大 10 台の SFF SAS/SATA/U.3 NVMe ドライブ（SAS4 トライモード RAID または HBA コントローラ経由）。オプションで最大 8 台の直接接続 U.2/U.3 NVMe ドライブを使用可能。
    - PCIe Gen5 x4 ごとに最大 16 台の E3.S 1T 直接接続 NVMe ドライブ。
- mLOM/OCP 3.0：
  - 背面パネルの追加接続用に、mLOM または OCP 3.0 カードを追加するために使用できる専用の PCIe 第 5 世代 x16 のスロット 1 個。
  - mLOM スロットは、10/25/50 と 40/100/200 Gbps Cisco VIC アダプタに柔軟に対応できます。
  - OCP 3.0 スロットは、mLOM インターポーザ経由で Intel X710 OCP デュアル 10GBase-T をサポートする完全なアウトオブバンド管理機能を装備。
- 電源：ホットプラグ可能な冗長プラチナおよびチタンのオプション：
  - プラチナ: 1050W DC、および 1600W AC

© 2025 Cisco and/or its affiliates. All rights reserved.

- チタン: 1200W AC、および 2300W AC

- 他のストレージ
  - サーバユーティリティ専用ベースボード管理コントローラ（BMC）FlexMMC（オンボード）。
  - HW RAID をサポートするデュアル M.2 SATA SSD（内蔵またはホットスワップ可能）。
- GPU：最大 3 個のシングルワイド GPU をサポート。

注:

- Cisco UCS シリーズ M8 サーバは、15000 シリーズセキュアブートアダプタのみをサポートします。
- Cisco UCS C220 M8 サーバには、Cisco Intersight インフラストラクチャファームウェアバージョン 4.3(6.250048) 以降が必要です。

Cisco UCS X215c M8 コンピューティングノードでサポートされている周辺機器の詳細なリストについては、Cisco UCS X215c 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。

Cisco UCS C240 M8 サーバ

2 RU、2 ソケットの Cisco UCS C240 M8 ラックサーバーは、I/O の柔軟性と大きなストレージ容量を提供します。このシリーズは最速の Intel® プロセッサを組み合わせており、多目的に使える汎用アプリケーションおよびインフラストラクチャサーバーです。AI、ビッグデータ分析、データベース、コラボレーション、仮想化、ハイパフォーマンスコンピューティングなど、幅広いワークロードで最先端のパフォーマンスと効率を実現します。

Cisco UCS C240 M8 サーバは、Intel Xeon® 6 CPU を組み込んで Cisco UCS ラックサーバポートフォリオの機能を拡張します。セキュリティ、パフォーマンス、効率を向上させ、Intel Trust Domain Extensions（TDX）、Intel Data Streaming Accelerator（DSA）、Intel QuickAssist Technology（QAT）、Intel Advanced Matrix Extensions（AMX）、および Intel In-Memory Analytics Accelerator（IAA）などの組み込みアクセラレータによりサステナビリティの目標を達成を支援します。

従来のサーバーを最新世代の Cisco UCS C240 M8 サーバーに移行・統合することで、電力と冷却、管理、メンテナンスといったサーバーの運用コスト（OpEx）を削減できます。

Cisco UCS C240 M8 サーバは、次の機能を提供します。

- 最大 2 個の Intel Xeon 6700P または 6500P プロセッサ（1 または 2）。
- メモリ：
  - 32 個の DDR4 DIMM スロット（CPU あたり 16 DIMM）：16、32、48、64、96、128、256GB DDR5、最大 6400 MT/s、最大 8TB のメモリ。
  - 32, 64GB MRDIMM、最大 8000 MT/s。
- PCIe 拡張：PCIe 5.0 スロットを最大 8 個、専用 24 Gbps RAID コントローラスロット 1 個、専用 mLOM/OCP 3.0 スロット 1 個
- RAID コントローラ：
  - SAS 4 または NVMe ハードウェア RAID をサポートする Cisco 24 Gbps モジュラトライモード RAID コントローラ。
  - Cisco 24 Gbps モジュール型トライモード SAS ホストバスアダプタ（HBA）。

© 2025 Cisco and/or its affiliates. All rights reserved.

- 内蔵ストレージ：
  - SAS4 トライモード RAID または HBA コントローラを介して最大 28 台の SFF SAS/SATA/U.3 NVMe ドライブ、オプションで最大 8 台の直接接続 U.2/U.3 NVMe ドライブ。
  - 最大 36 台の E3.S 1T 直接接続 NVMe ドライブ。
  - 最大 16 台の LFF SAS HDD とオプションで 4 台の背面 SFF HDD/SSD。
- mLOM/OCP 3.0：背面パネルの追加接続用に、mLOM または OCP 3.0 カードを追加するために使用できる専用の PCIe 第 5 世代 x16 のスロット 1 個。
  - mLOM スロットは、10/25/50 と 40/100/200 Gbps Cisco VIC アダプタに柔軟に対応できます。
  - OCP 3.0 スロットは、mLOM インターポーザを介して Intel X710 OCP デュアル 10GBase-T をサポートする完全なアウトオブバンド管理機能を備えています。
- 電源：ホットプラグ可能な冗長プラチナおよびチタンのオプション:
  - プラチナ: 1050W DC、および 1600W AC
  - チタン: 1200W AC、および 2300W AC
- 他のストレージ
  - サーバユーティリティ専用ベースボード管理コントローラ（BMC）FlexMMC（オンボード）。
  - HW RAID をサポートするデュアル M.2 SATA SSD（内蔵またはホットスワップ可能）。
- GPU：最大 3 つのダブル幅 GPU または 8 つのシングル幅 GPU をサポート

(注)

- Cisco UCS シリーズ M8 サーバは、15000 シリーズセキュアブートアダプタのみをサポートします。
- Cisco UCS C240 M8 サーバには、Cisco Intersight インフラストラクチャファームウェアバージョン 4.3(6.250048) 以降が必要です。

Cisco UCS C240 M8 コンピューティングノードでサポートされている周辺機器の詳細なリストについては、Cisco UCS C240 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 M8 サーバファームウェアリリース 5.3(0.250001) の新しいハードウェア

Cisco UCS X215c M8 コンピューティングノードでは次の第 5 世代 AMD EPYC CPU をサポートします。

- UCSX-CPU-A9655
- UCSX-CPU-A9555
- UCSX-CPU-A9355
- UCSX-CPU-A9135
- UCSX-CPU-A9575F

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco UCS X215c M8 コンピューティングノードでの UCSC-GPU-MI210 GPU のサポート。
Cisco UCS X215c M8 コンピューティングノードで、第 5 世代 AMD EPYC? CPU 用に次の DDR5-6400 MT/s DIMM をサポートします。 • UCS-MRX32G1RE5 • UCS-MRX64G2RE5
Cisco UCS X215c M8 コンピューティングノードの第 4 世代 AMD EPYC? CPU 用に次の DDR5-5600 MT/s DIMM をサポートします。 • UCSX-MR128G2RG3

C シリーズ M8 サーバファームウェアリリース 4.3(5.250001) の新しいハードウェア機能

Cisco UCS C245 M8 サーバーで次の第 5 世代 AMD EPYC CPU をサポートします。 • UCS-CPU-A9655 • UCS-CPU-A9555 • UCS-CPU-A9355 • UCS-CPU-A9135 • UCS-CPU-A9575F
Cisco UCS C225 M8 サーバーで次の第 5 世代 AMD EPYC CPU をサポートします。 • UCS-CPU-A9655 • UCS-CPU-A9555 • UCS-CPU-A9355 • UCS-CPU-A9135 • UCS-CPU-A9575F
第 4 世代および第 5 世代の AMD EPYC プロセッサを搭載した Cisco UCS C225 M8 および C245 M8 サーバーで、次の Cisco Tri-Mode M1 24G RAID ストレージコントローラをサポートします。 • UCSC-RAID-M1L16 • UCSC-RAID-MP1L32
Cisco UCS C245 M8 サーバーで UCSC-GPU-MI210 GPU をサポートします。
Cisco UCS C225 M8 および C245 M8 サーバーでは、第 5 世代 AMD EPYC™ CPU 用に、次の DDR5-6400 MT/s DIMM をサポートします。 • UCS-MRX32G1RE5 • UCS-MRX64G2RE5
Cisco UCS C245 M8 サーバーでは、第 5 世代 AMD EPYC™ CPU 用に、次の DDR5-6400 MT/s DIMM をサポートします。 • UCS-MRX96G2RF5

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco UCS C225 M8 および C245 M8 サーバーでは、第 4 世代 AMD EPYC™ CPU 用に、次の DDR5-5600 MT/s DIMM をサポートします。

- UCS-MR128G2RG3

X シリーズ M8 5.3(0.240016) サーバファームウェアの新しいハードウェア

Cisco UCS X215c M8 コンピューティングノード

Cisco UCS X シリーズモジュラシステムは、データセンターを簡素化し、最新のアプリケーションの予測不可能なニーズに対応すると同時に、従来のスケールアウトやエンタープライズワークロードにも対応します。維持するサーバータイプの数が減り、複雑さが軽減されるので、運用の効率性と俊敏性が向上します。Cisco UCS X シリーズには Cisco Intersight™ クラウド運用プラットフォームが搭載されているため、思考の矛先を管理からビジネス成果へと変えることができます。使用するハイブリッドクラウドインフラストラクチャは、クラウドからワークロードに合わせて組み合わせて成形し、継続的に最適化できます。

Cisco UCS X215c M8 コンピューティングノードは、Cisco UCS X シリーズモジュラシステムに統合されています。7 ラックユニット（7RU）Cisco UCS X9508 シャーシには、最大 8 個のコンピューティングノードを配置でき、ラックユニットあたりのコンピューティング、IO、およびストレージの密度は業界で最も高い 1 つです。

Cisco UCS X215c M8 コンピューティングノードは、次の機能を提供します。

- CPU：最大 2 個の第 4 世代 AMD EPYC プロセッサ（プロセッサあたり最大 128 コア）。
- メモリ：
  - 24 基の DIMM スロット（CPU ソケットあたり 12 個の DIMM）、最大 4800 MT/s DDR5。
  - 最大 6 TB のキャパシティ 。
- ストレージ：最大 6 台のホットプラグ可能なソリッドステートドライブ（SSD）、または不揮発性メモリエクスプレス（NVMe）2.5 インチドライブで、エンタープライズクラスの Redundant Array of Independent Disk（RAID）、または各レーンの PCIe Gen 4 接続と最大 2 台の M.2 SATA または NVMe ドライブを搭載した 4 台のパススルーコントローラを選択可能。
- オプションの前面メザニン GPU モジュール：Cisco UCS 前面メザニン GPU モジュールは、最大 2 つの U.2 または U.3 NVMe ドライブと 2 つの HHHL GPU をサポートするパッシブ PCIe Gen 4 前面メザニンオプションです。
- mLOM 仮想インターフェイスカード：
  - Cisco UCS 仮想インターフェイスカード（VIC）15420 は、サーバーのモジュール型 LAN on Motherboard（mLOM）スロットを占有し、サーバーあたり 100 Gbps 接続に対して各シャーシのインテリジェントファブリックモジュール（IFM）に最大 50 Gbps（2 x 25 Gbps）で接続できます。
  - Cisco UCS 仮想インターフェイスカード（VIC）15230 は、サーバのモジュラ型 LAN オンマザーボード（mLOM）スロットを占有でき、サーバあたり 100 Gbps 接続に対して各シャーシのインテリジェントファブリックモジュール（IFM）に最大 100 Gbps で接続できます。
- オプションのメザニンカード：
  - オプションの Cisco UCS 仮想インターフェイスカード（VIC）15422 は、シャーシの下部にあるサーバーのメザニンスロットに装着できます。付属のブリッジカードは、IFM コネクタを介してこの VIC の 100 Gbps（4 x 25 Gbps）のネットワーク接続を拡張し、合計帯域幅を VIC 15420 および 15422 あたり 100 Gbps（サーバーあたり合計 200 Gbps）にします。IFM 接続に加えて、VIC 15422 I/O コネクタは Cisco UCS X-Fabric テクノロジーにリンクします。

© 2025 Cisco and/or its affiliates. All rights reserved.

- X-Fabric の Cisco UCS PCI Mezz カードは、シャーシの下部にあるサーバーのメザニンスロットに装着できます。このカードの I/O コネクタは Cisco UCS X-Fabric モジュールにリンクし、X440p PCIe ノードへの接続を可能にします。

- セキュリティ: セキュアブートシリコンルートオブトラスト FPGA、ACT2 偽造防止規定、およびオプションのトラステッドプラットフォームモデル（TPM）が含まれます。

Cisco UCS X215c M8 コンピューティングノードでサポートされている周辺機器の詳細なリストについては、Cisco UCS X215c 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。

注：Cisco UCS X215c M8 コンピューティングノードは、14000 シリーズおよび 15000 シリーズセキュアブート VIC アダプタのみをサポートします。

X シリーズ M7 サーバファームウェアリリース 5.3(0.240016)

UCSX-210C-M7 コンピューティングノードでの UCSX-GPU-H100-NVL および UCSX-GPU-L4-MEZZ GPU のサポートが追加されました。

C シリーズ M8 サーバファームウェアリリース 4.3(5.240021) の新しいハードウェア機能

Cisco UCS C225 M8 サーバ

Cisco UCS C225 M8 サーバーは、多目的に使える、インフラおよびアプリケーション向けの汎用サーバーです。この高密度の 1RU、単一ソケットのラックサーバーは、仮想化、コラボレーション、ベアメタルアプリケーションなど、多様なワークロードで業界をリードするパフォーマンスと効率性を実現します。

Cisco UCS C225 M8 サーバーは、Cisco UCS ラックサーバーポートフォリオの機能を拡張します。AMD のチップレットアーキテクチャを使用して設計されたソケットあたりのコア数が 100% 増加した第 4 世代 AMD EPYC™ プロセッサを駆動します。AMD Infinity Guard などの高度な機能により、コンピューティング集約型アプリケーションのパフォーマンスが大幅に向上し、電力効率やコスト効率などのメリットが得られます。

Cisco UCS C225 M8 ラックサーバは、スタンドアロンサーバとして、または Cisco Intersight™ または Cisco UCS Manager によって管理される Cisco Unified Computing System® の一部として展開して、Cisco® 標準ベースのユニファイドコンピューティングイノベーションを活用してコストを削減でき、総所有コスト (TCO) を高め、ビジネスの機敏性を向上させます。

C225 M8 ラックサーバは、Cisco UCS AMD ラックサーバのポートフォリオに多くの新しい革新をもたらします。高速 I/O、DDR5 メモリバス、および拡張ストレージ機能用の PCIe Gen 5.0 の導入により、サーバーのパフォーマンスと効率が大幅に向上し、アプリケーションのパフォーマンスが最適化されます。

Cisco UCS C225 M8 サーバーの主な機能は次のとおりです。

- ソケットあたり最大 128 コアの第 4 世代 AMD EPYC CPU 1 基をサポート
- 最大 12 枚の DDR5 DIMM、128 GB DIMM を使用して最大 1.5 TB のキャパシティ。
- 最大 4800 MT/秒の DDR5 メモリ
- 最大 3 つの PCIe 4.0 スロットまたは最大 2 つの PCIe 5.0 スロット、およびモジュール型 LAN on Motherboard（mLOM） / OCP スロット 3.0
- Cisco UCS VIC 15000 シリーズアダプタとサードパーティのホストの NIC オプションのサポート
- UCS C225 M8S シャーシ：最大 10 台の SAS/SATA または NVMe ディスクドライブ

© 2025 Cisco and/or its affiliates. All rights reserved.

- 新しいトライモード RAID コントローラは、SAS4 または NVMe ハードウェア RAID をサポート
- 最大 4 つの直接接続 NVMe SSD

- UCS C225 M8N シャーシ：最大 10 台の直接接続 NVMe SSD
  - PCIe Gen4 x4 に接続された 10 台の NVMe ドライブすべて
- M.2 起動用ドライブ （オプション）
  - ハードウェア RAID を備えた最大 2 台の 960 GB SATA M.2 ドライブ、または
  - NVMe ハードウェア RAID を備えた最大 2 台の 960GB NVMe M.2 ドライブ
- 最大 3 個の GPU をサポート
- ハイブリッドモジュラ LOM / OCP 3.0
  - 背面パネルの追加接続用に、mLOM または OCP 3.0 カードを追加するために使用できる専用の 4.0 世代 x16 のスロット x 1
  - mLOM は、PCIe スロットを消費せずに Cisco UCS 仮想インターフェイスカード（VIC）許可します。クワッドポート 10/25/50 Gbps または、デュアルポート 40/100/200 Gbps ネットワーク接続をサポートします。
  - OCP 3.0 スロットは、一部のアダプターに対して、完全なアウトオブバンド管理を可能にします

Cisco UCS C225 M8 サーバでサポートされる周辺機器の詳細なリストについては、Cisco UCS C225 M8 SFF ラックサーバ仕様書を参照してください。

注：Cisco UCS C225 M8 サーバは、14000 シリーズおよび 15000 シリーズセキュアブート VIC アダプタのみをサポートします。

Cisco UCS C245 M8 サーバ

Cisco UCS C245 M8 サーバでの次の UCSC-GPU-H100-NVL GPU のサポートを追加しました。

X シリーズ M7 サーバファームウェア 5.2(2.240053) および B シリーズ M7 および M6 サーバファームウェア 5.2(2.240051) の新しいハードウェア機能

Cisco UCS X410c M7 コンピューティングノードで次の DIMM をサポートします：UCSX-MRX96G2RF3

Cisco UCS X410c M7 および Cisco UCS X210c M7 コンピューティングノードで、次のグラフィック処理をサポートします：UCSX-GPU-L40S

Cisco UCS X210c M7、X410c M7、X210c M6 コンピューティングノードでの次のトラステッドプラットフォームモジュールをサポートします：UCS-TPM-002D

Cisco UCS X210c コンピューティングノードでは、第 5 世代 Intel® Xeon® スケーラブルプロセッサがサポートされています。

- UCSX-CPU-I4510T - Intel® Xeon® Silver 4510T プロセッサ
- UCSX-CPU-I4510 - Intel® Xeon® Silver 4510 プロセッサ

© 2025 Cisco and/or its affiliates. All rights reserved.

- UCSX-CPU-I4509Y – Intel® Xeon® Silver 4509Y プロセッサ
- UCSX-CPU-I3508U：Intel® Xeon® Bronze 3508U プロセッサ

B シリーズ M6 サーバファームウェア 5.2(2.240051) の新しいハードウェア機能

Cisco UCS B200 M6 サーバでの次のトラステッドプラットフォームモジュールのサポート： UCS-TPM-002D

X シリーズ M7 ファームウェア 5.2(1.240010) の新しいハードウェアサポート

サーバファームウェアリリースバージョン 5.2(1.240010) を搭載した Cisco UCS X210c コンピューティングノードで、第 5 世代 Intel® Xeon® スケーラブルプロセッサがサポートされています。

- UCSX-CPU-I8592V：Intel® Xeon® Platinum 8592V プロセッサ
- UCSX-CPU-I8592+：Intel® Xeon® Platinum 8592+ プロセッサ
- UCSX-CPU-I8581V – Intel® Xeon® Platinum 8581V プロセッサ
- UCSX-CPU-I8580：Intel® Xeon® Platinum 8580 プロセッサ
- UCSX-CPU-I8571N – Intel® Xeon® Platinum 8571 プロセッサ
- UCSX-CPU-I8570 – Intel® Xeon® Platinum 8570 プロセッサ
- UCSX-CPU-I8568Y+：Intel® Xeon® Platinum 8568Y+ プロセッサ
- UCSX-CPU-I8562Y+：Intel® Xeon® Platinum 8562Y+ プロセッサ
- UCSX-CPU-I8558U – Intel® Xeon® Platinum 8558U プロセッサ
- UCSX-CPU-I8558P – Intel® Xeon® Platinum 8558P プロセッサ
- UCSX-CPU-I8558 – Intel® Xeon® Platinum 8558 プロセッサ
- UCSX-CPU-I6554S – – Intel® Xeon® Gold 6554S プロセッサ
- UCSX-CPU-I6548Y+：Intel® Xeon® Gold 6548Y+ プロセッサ
- UCSX-CPU-I6548N：Intel® Xeon® Gold 6548N プロセッサ
- UCSX-CPU-I6544Y：Intel® Xeon® Gold 6544Y プロセッサ
- UCSX-CPU-I6542Y – Intel® Xeon® Gold 6542 プロセッサ
- UCSX-CPU-I6538Y+：Intel® Xeon® Gold 6538Y+ プロセッサ
- UCSX-CPU-I6538N – Intel® Xeon® Gold 6538N プロセッサ
- UCSX-CPU-I6534：Intel® Xeon® Gold 6534 プロセッサ
- UCSX-CPU-I6530：Intel® Xeon® Gold 6530 プロセッサ
- UCSX-CPU-I6526Y：Intel® Xeon® Gold 6526Y プロセッサ
- UCSX-CPU-I5520+ – Intel® Xeon® Gold 5520+ プロセッサ
- UCSX-CPU-I5515+ – Intel® Xeon® Gold 5515+ プロセッサ
- UCSX-CPU-I5512U – Intel® Xeon® Gold 5512U プロセッサ

© 2025 Cisco and/or its affiliates. All rights reserved.

- UCSX-CPU-I4516Y+ - Intel® Xeon® Silver 4516Y+ プロセッサ
- UCSX-CPU-I4514Y - Intel® Xeon® Silver 4514Y プロセッサ

C シリーズ M5 ファームウェア 4.3(3.240022) の新しいハードウェアサポート

サーバファームウェアバージョン 4.3(3.240022) を搭載した Cisco UCS C220 M7 および C240 M7 サーバで、次の第 5 世代 Intel® Xeon® スケーラブルプロセッサをサポートします。

- UCS-CPU-I8592V：Intel® Xeon® Platinum 8592V プロセッサ
- UCS-CPU-I8592+：Intel® Xeon® Platinum 8592+ プロセッサ
- UCS-CPU-I8580：Intel® Xeon® Platinum 8580 プロセッサ
- UCS-CPU-I8568Y+：Intel® Xeon® Platinum 8568Y+ プロセッサ
- UCS-CPU-I8562Y+：Intel® Xeon® Platinum 8562Y+ プロセッサ
- UCS-CPU-I8558P：Intel® Xeon® Platinum 8558P プロセッサ
- UCS-CPU-I8558：Intel® Xeon® Platinum 8558 プロセッサ
- UCS-CPU-I6554S - Intel® Xeon® Gold 6554S プロセッサ
- UCS-CPU-I6548Y+：Intel® Xeon® Gold 6548Y+ プロセッサ
- UCS-CPU-I6548N：Intel® Xeon® Gold 6548N プロセッサ
- UCS-CPU-I6544Y：Intel® Xeon® Gold 6544Y プロセッサ
- UCS-CPU-I6542Y：Intel® Xeon® Gold 6542Y プロセッサ
- UCS-CPU-I6538Y+：Intel® Xeon® Gold 6538Y+ プロセッサ
- UCS-CPU-I6534：Intel® Xeon® Gold 6534 プロセッサ
- UCS-CPU-I6530：Intel® Xeon® Gold 6530 プロセッサ
- UCS-CPU-I6526Y：Intel® Xeon® Gold 6526Y プロセッサ
- UCS-CPU-I5520+：Intel® Xeon® Gold 5520+ プロセッサ
- UCS-CPU-I5515+：Intel® Xeon® Gold 5515+ プロセッサ
- UCS-CPU-I4516Y+：Intel® Xeon® Silver 4516Y+ プロセッサ
- UCS-CPU-I4514Y：Intel® Xeon® Silver 4514Y プロセッサ

サポート対象の GPU

上記の CPU を搭載した次の GPU カードのサポート：

- Cisco UCS C240 M7 サーバでの Data Center GPU Flex 170、FH-3/4L、150W PCIe のサポート
- Cisco UCS C220 M7 および C240 M7 サーバーでの Data Center GPU Flex 140、HHHL、75W PCIe のサポート

© 2025 Cisco and/or its affiliates. All rights reserved.

DDR5 5600 MT/s DIMM のサポート

サーバファームウェアバージョン 5.2(1.240010) を搭載した Cisco UCS X410c M7 および X210c M7 コンピューティングノードで、次の 5600 DIMM をサポートします。

- UCSX-MRX16G1RE3 - 16GB DDR5-5600 RDIMM 1Rx8（16Gb）
- UCSX-MRX32G1RE3 - 32GB DDR5-5600 RDIMM 1Rx4（16GB）
- UCSX-MRX64G2RE3 - 64GB DDR5-5600 RDIMM 2Rx4（16GB）
- UCSX-MRX96G2RF3 - 96GB DDR5-5600 RDIMM 2Rx4（24GB）
- UCSX-MR128G4RE3 - 128GB DDR5-5600B RDIMM 4Rx4（16GB）
- UCSX-MR256G8RE3 - 256GB DDR5-5600 RDIMM 8Rx4 (16Gb)

サーバファームウェアバージョン 4.3(3.240022) を搭載した Cisco UCS C240 M7 および C220 M7 サーバで、次の 5600 DIMM をサポートします。

- UCS-MRX16G1RE3 - 16GB DDR5-5600 RDIMM 1Rx8（16Gb）
- UCS-MRX32G1RE3 - 32GB DDR5-5600 RDIMM 1Rx4（16Gb）
- UCS-MRX64G2RE3 - 64GB DDR5-5600 RDIMM 2Rx4（16GB）
- UCS-MRX96G2RF3 - 96GB DDR5-5600 RDIMM 2Rx4（24GB）
- UCS-MR128G4RE3 - 128GB DDR5-5600 RDIMM 4Rx4（16GB）
- UCS-MR256G8RE3 - 256GB DDR5-5600 RDIMM 8Rx4 (16Gb)

X シリーズ M7 ファームウェア 5.2(0.230092) の新しいハードウェアサポート

Cisco UCS X シリーズサーバで、次の Cisco UCS VIC 15000 シリーズセキュアブート対応 mLOM アダプタをサポートします。

UCSX-ML-V5D200GV2：X シリーズ M6 および M7 サーバ上の Cisco UCS VIC 15230 (2x100G or 4x25G) mLOM。

（注）

上記のハードウェアは、インフラストラクチャファームウェアバージョン 4.3(2.230129) 以降と互換性があります。

新しいハードウェアサポートの詳細については、「Intersight 管理モードのサポートされるハードウェア」を参照してください。

X シリーズ M7 ファームウェア 5.2(0.230041) の新しいハードウェアサポート

Cisco UCS X210c M7 コンピューティングノードで UCSX-M2-PT-FPN（M.2 NVMe コントローラ）をサポートします。

Cisco UCS X210c M7 および UCS X410c M7 コンピューティングノードで次のグラフィック処理をサポートします。

- UCSC-GPU-H100-80
- UCSC-GPU-L40
  - UCSC-GPU-L4

© 2025 Cisco and/or its affiliates. All rights reserved.

- UCSC-GPU-FLEX140
- UCSC-GPU-FLEX170

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

C シリーズ M7 サーバーファームウェアリリース 4.3(4.242038) の新しいハードウェア機能

以下の Cisco トライモード M1 24G RAID および HBA コントローラのサポート：

- Cisco UCSC-C220-M7 サーバ上の UCSC-HBA-M1L16 および UCSC- RAID-M1L16
- Cisco UCSC-C240-M7 サーバ上の UCSC-HBA-M1L16 および UCSC- RAID-MP1L32

Cisco Trimode M1 24G RAID および HBA コントローラの利点：

- エンタープライズキー管理（EKMS）を使用してリモートキーを管理し、データの物理的なセキュリティを強化します。
- Distributed Management Task Force（DMTF）の Redfish スキーマを使用して、ストレージソフトウェアアーキテクチャまたはスタックの変更からの独立性を確保します。
- アウトオブバンド管理により、新しいベンダーとアダプタを迅速に統合できます。
- 最大ドライブ容量の 5% は、時間の経過に伴うドライブサイズのわずかなバリアンスを許容するために予約済みです。

C シリーズ M8 サーバファームウェアリリース 4.3(4.241014) の新しいハードウェア機能

Cisco UCS C245 M8 ラックサーバ

Cisco UCS C245 M8 ラックサーバーは、Cisco UCS ラックサーバーポートフォリオの機能を拡張します。これは、前世代と比較してソケットあたりのコア数が 2 倍になり、AMD のチップレットアーキテクチャを使用して設計された第 4 世代 AMD EPYC™ プロセッサを駆動します。AMD Infinity Guard などの高度な機能により、コンピューティング集約型アプリケーションのパフォーマンスが大幅に向上し、電力効率やコスト効率などのメリットが得られます。

高速 I/O、DDR5 メモリバス、および拡張ストレージ機能用の PCIe Gen 5.0 拡張スロットの導入により、サーバーはパフォーマンスと効率を大幅に向上させ、アプリケーションのパフォーマンスを大幅に向上させます。

次のようなサーバの機能があります。

- CPU：最大 256 CPU コア（ソケットあたり 128 コア）を駆動するように設計されたサーバで、最大 2 つの第 4 世代 AMD EPYC™ CPU をサポートします。
- ストレージ：最大 24 枚の DDR5 DIMM スロット、256 GB DIMM を使用して最大 6 TB の容量（ソケットあたり 12 枚の DIMM を使用）
- メモリ：最大 4800 MT/秒の DDR5 メモリ
- 最大 8 個の PCIe Gen 4.0 スロットまたは最大 4 個の PCIe Gen 5.0 スロット、およびマザーボード上のハイブリッドモジュラー LAN（mLOM）/OCP 3.0 スロット
- アダプタ：Cisco UCS VIC 15000 シリーズアダプタと複数のサードパーティの NIC オプションをサポート

© 2025 Cisco and/or its affiliates. All rights reserved.

- 最大 28 台のホットスワップ可能な小型フォームファクタ（SFF）SAS/SATA または NVMe ドライブ（最大 8 台の直接接続 NVMe ドライブ）
  - 新しいトライモード RAID コントローラは、SAS4 と NVMe ハードウェア RAID をサポート
- M.2 起動用ドライブ （オプション）
  - ハードウェア RAID を備えた最大 2 台の 960GB SATA M.2 ドライブのサポート
  - NVMe ハードウェア RAID を備えた最大 2 台の 960GB NVMe M.2 ドライブ
- GPU：最大 8 個の GPU をサポート
- モジュラ LOM / OCP 3.0
  - 背面パネルの追加接続用に、mLOM または OCP 3.0 カードを追加するために使用できる専用の PCIe 4 世代 x16 のスロット 1 個
  - 10/25/50 Gbps のクワッドポートまたは 40/100/200 Gbps のデュアルネットワーク接続をサポートし、PCIe スロットを使用せずに、Cisco UCS 仮想インターフェイスカード（VIC）をスロットで搭載可能
  - OCP 3.0 スロットは、一部のアダプターに対して、完全なアウトオブバンド管理を可能にします

サーバにバンドルされているサブコンポーネントの詳細については、「Cisco UCS C245 M8 サーバ仕様シート」を参照してください。

C シリーズ M6 および M7 サーバファームウェアリリース 4.3 (4.240152) の新しいハードウェア機能

Cisco UCS C240 M7 サーバーでの次のグラフィックスプロセッシングユニットのサポート：

- UCSC-GPU-L40S

Cisco UCS C220 M6 および C240 M6 サーバーでの次のグラフィック処理ユニットのサポート：

- UCSC-GPU-L4

Cisco UCS C220 M7、C240 M7、C220 M6、および C240 M6 サーバーでの次のトラステッドプラットフォームモジュールのサポート：

- UCS-TPM-002D

Cisco UCS C225 M6、および C245 M6 サーバーでの次のトラステッドプラットフォームモジュールのサポート：

- UCS-TPM2-002D

Cisco UCS C220 M7 および C240 M7 サーバでの次の第 5 世代 Intel® Xeon® スケーラブルプロセッサのサポート：

- UCS-CPU-I4510T：Intel® Xeon® Silver 4510T プロセッサ
- UCS-CPU-I4510：Intel® Xeon® Silver 4510 プロセッサ
- UCS-CPU-I4509Y：Intel® Xeon® Silver 4509Y プロセッサ
- UCS-CPU-I3508U：Intel® Xeon® Bronze 3508U プロセッサ

© 2025 Cisco and/or its affiliates. All rights reserved.

C シリーズファームウェア 4.3(2.230270) の新しいハードウェアサポート

Cisco UCS C シリーズサーバで、次の Cisco UCS VIC 15000 シリーズセキュアブート対応 mLOM アダプタをサポートします。

- UCSC-M-V5D200GV2：C シリーズ M6 および M7 サーバ上の Cisco UCS VIC 15237（2x40/100/200G）mLOM。
- UCSC-M-V5Q50GV2：C シリーズ M6 および M7 サーバ上の Cisco UCS VIC 15427（4x10/25/50G）mLOM。

（注）

上記のハードウェアは、インフラストラクチャファームウェアバージョン 4.3(2.230129) 以降と互換性があります。

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

C シリーズファームウェア 4.3(2.230207) の新しいハードウェアサポート

Cisco UCS C シリーズ M6 および M7 サーバで、次の Cisco UCS VIC 15000 シリーズセキュアブート対応 PCIe アダプタをサポートします。

- UCSC-P-V5D200G - Cisco UCS VIC 15235 2x40/100/200G
- UCSC-P-V5Q50G - Cisco UCS VIC 15425 4x10/25/50G

（注）

上記のハードウェアは、インフラストラクチャファームウェアバージョン 4.3(2.230117) 以降と互換性があります。

次のグラフィックスプロセッシングユニットのサポート：

- Cisco UCS C240 M7 サーバの UCSC-GPU-H100-80
- Cisco UCS C240 M7 サーバの UCSC-GPU-L40
- Cisco UCS C シリーズ M7 サーバの UCSC-GPU-L4
- Cisco UCS C シリーズ M7 サーバの UCSC-GPU-FLEX140
- Cisco UCS C240 M7 サーバの UCSC-GPU-FLEX170

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

C シリーズファームウェア 4.3（1.230097）での新しいハードウェアサポート

Cisco UCS C220 M7 および C240 M7 サーバをサポートします。

C シリーズ M7 サーバでの次のグラフィックスプロセッシングユニットのサポート：

- UCSC-GPU-A16
- UCSC-GPU-A100-80

詳細については、Intersight 管理モードのサポート対象ハードウェアを参照してください。

© 2025 Cisco and/or its affiliates. All rights reserved.

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。

X シリーズ M8 5.4（0.250040）、5.4（0.250044）と M7 5.4（0.250040）、および C シリーズ 4.3（6.250044）サーバファームウェアリリースの Security 修正 - なし

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 4.3(5.250033) のセキュリティ修正

C シリーズ M5 サーバファームウェアリリース 5.4(0.250034) のセキュリティ修正

欠陥 ID - CSCwm73565

Intel CPU と BIOS を搭載した Cisco UCS B シリーズ M5 サーバは、次の Common Vulnerabilities and Exposures (CVE) ID で特定された脆弱性の影響を受けます。

- CVE-2024-28047：一部の Intel® プロセッサの UEFI ファームウェアにおける不適切な入力検証により、特権ユーザーがローカルアクセスを通じて情報漏洩やサービス拒否を実行できる可能性があります。

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 4.3(5.250030) のセキュリティ修正

欠陥 ID - CSCwn63691

Cisco UCS C225 M6 および C245 M6 サーバは、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ます。

- CVE-2024-56161：AMD CPU ROM マイクロコードパッチローダーでの不適切な署名検証により、ローカル管理者権限を持つ攻撃者が悪意のある CPU マイクロコードをロードし、AMD SEV-SNP で実行されている機密性のあるゲストの機密性と完全性を失う権限。
- CVE-2024-21925：AmdPspP2CmboxV2 ドライバ内での入力検証が不適切なため、権限を持つ攻撃者が SMRAM を上書き、任意のコードが実行される可能性があります。
- CVE-2024-21924：AmdPlatformRasSspSmm ドライバ内の SMM コールアウトの脆弱性により、リング 0 の攻撃者がブートサービスハンドラを変更し、任意のコードが実行される可能性があります。

X シリーズ 5.3(0.240016) および B シリーズ 5.3(0.240014) サーバファームウェアリリースのセキュリティ修正

不具合識別子：CSCwk62723

Cisco UCS B シリーズブレードサーバーシリアルオーバー LAN（SOL）および）Cisco UCS X シリーズコンピュートシリアルオーバー LAN（SOL）には,次の Common Vulnerabilities and 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-2024-6387：OpenSSH のサーバー（sshd）でセキュリティ回帰（CVE-2006-5051）が検出されました。競合状態が存在するため、sshd で特定の信号が危険な仕方で処理される可能性があります。この脆弱性は、認証されていないリモートの攻撃者が、指定された期間内に認証に失敗したときにエクスプロイトされる可能性があります。

© 2025 Cisco and/or its affiliates. All rights reserved.

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。

X シリーズ M7 5.2（2.240074）、X シリーズ M6 5.2（2.240073）、および B シリーズ M6 5.2（2.240073）ファームウェアリリースのセキュリティ修正

不具合識別子 ：CSCwk62723

Cisco UCS B シリーズブレードサーバーシリアルオーバー LAN（SOL）および）Cisco UCS X シリーズコンピュートシリアルオーバー LAN（SOL）には,次の Common Vulnerabilities and 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-2024-6387：OpenSSH のサーバー（sshd）でセキュリティ回帰（CVE-2006-5051）が検出されました。競合状態が存在するため、sshd で特定の信号が危険な仕方で処理される可能性があります。この脆弱性は、認証されていないリモートの攻撃者が、指定された期間内に認証に失敗したときにエクスプロイト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。

X シリーズ M6 サーバ 5.2(0.230127)、B シリーズサーバ 5.2(0.230127)、および C シリーズ M6 サーバ 4.3(2.240002) のセキュリティ修正

不具合 ID：CSCwh68315

Cisco UCS B シリーズ M6 サーバ、UCS C シリーズ M6 サーバ、UCS X シリーズ M6 コンピューティングノードには、以下の一般的な脆弱性およびエクスポージャ（CVE）ID で識別される脆弱性の影響を受ける Intel® CPU が含まれています：

- CVE-2023-23583：プロセッサ命令のシーケンスにより、一部の Intel® プロセッサで予期しない動作が発生し、認証されたユーザーがローカルアクセスを介した特権の昇格、情報開示、およびサービス妨害を可能にする可能性があります。

B シリーズ M6 5.2(1.240010) および C シリーズ 4.3(3.240022)、X シリーズ 5.2(1.240010) M6 および M7 サーバのセキュリティ修正

不具合 ID：CSCwh58728

Cisco UCS Manager 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-2023-38408：9.3p2 より前の OpenSSH の ssh-agent の PKCS#11 機能には、信頼できる検索パスが不十分であり、エージェントが攻撃者が制御するシステムに転送された場合にリモートでコードが実行される。（/usr/lib のコードは、ssh-agent にロードするのに必ずしも安全ではありません）。

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。

© 2025 Cisco and/or its affiliates. All rights reserved.

C シリーズ M5 サーバファームウェアリリース 4.3(2.250016) のセキュリティ修正

欠陥 ID - CSCwm73565

Cisco UCS M5 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ます。

- CVE-2024-28047：一部の Intel® プロセッサの UEFI ファームウェアにおける不適切な入力検証により、特権ユーザーがローカルアクセスを通じて情報漏洩やサービス拒否を実行できる可能性があります。

C シリーズ M5 サーバファームウェアリリース 4.3(2.240090) のセキュリティ修正

不具合 ID：CSCwk77757

Cisco UCS M5 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ます。

- CVE-2024-24853：一部の Intel(R) プロセッサでのエグゼクティブモニターと SMI 転送モニター（STM）間の遷移の誤った動作順序により、特権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-2024-21781：一部の Intel® プロセッサの UEFI ファームウェアにおける不適切な入力検証により、特権ユーザーがローカルアクセスを通じて情報漏洩やサービス拒否を実行できる可能性があります。

障害 ID：CSCwi21160

Cisco UCS サーバーには、次の共通脆弱性識別子（Common Vulnerabilities and 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-2019-1543 -ChaCha20-Poly1305 は AEAD 暗号であり、すべての暗号化操作に一意のナンス入力が必要です。RFC 7539 では、ナンス値（IV）は 96 ビット（12 バイト）である必要があると指定しています。OpenSSL では、可変ナンス長を使用でき、12 バイト未満の場合は、ナンスを 0 バイトで前面に埋め込むことができます。ただし、最大 16 バイトのナンスを誤って設定することも可能になっています。この場合、最後の 12 バイトだけが有効で、そこまでのバイトは無視されます。この暗号を使用するための要件は、ナンス値が一意であることです。再利用されたナンス値を使用して暗号化されたメッセージは、重大な機密性および完全性攻撃の影響を受けます。アプリケーションがデフォルトのナンス長を 12 バイトより長く変更し、新しい値を新しい一意のナンスであると予期して、ナンスの先頭バイトに変更を加えた場合、そのようなアプリケーションは、再利用されたナンスで意図せずにメッセージを暗号化する可能性があります。さらに、長いナンスで無視されたバイトは、この暗号の完全性保証の対象にはなりません。無視された長いナンスの先頭バイトの整合性に依存するアプリケーションは、さらに影響を受ける可能性があります。SSL/TLS を含め、この暗号の内部での OpenSSL 使用は、そのような使用では長いナンス値を設定しないため、安全です。ただし、この暗号を直接使用し、デフォルト以外のナンス長を 12 バイトよりも長く設定するユーザーアプリケーションは脆弱になる可能性があります。OpenSSL バージョン 1.1.1 および 1.1.0 は、この問題の影響を受けます。影響を受ける展開の範囲が限られているため、その重大度は低いと評価されており、現時点では新しいリリースは作成されていません。OpenSSL 1.1.1c で修正済み（1.1.1-1.1.1b が影響を受けます）。OpenSSL 1.1.0k で修正済み（1.1.0-1.1.0j が影響を受けます）。
- CVE-2019-1547：通常、OpenSSL の楕円曲線グループには常に共通因子が存在し、これはサイドチャネルに耐性のあるコードパスで使用されます。ただし、場合によっては、（名前付き曲線を使用する代わりに）明示的なパラメータを使用してグループを作成することもできます。このような場合、該当するグループには共同因子が存在しない可能性があります。これは、すべてのパラメータが既知の曲線と一致する場合でも発生する可能性があります。このような曲線が使用されている場合、

© 2025 Cisco and/or its affiliates. All rights reserved.

OpenSSL は非サイドチャネルの耐性のあるコードパスにフォールバックし、ECDSA 署名操作中に完全なキーの回復が発生する可能性があります。脆弱性を利用するために、攻撃者は、共通因子のない明示的なパラメータが、libcrypto を使用するアプリケーションによって使用されている多数の署名の作成に対応することになります。疑義を避けるために付言すると、明示的なパラメータが使用されないため、libssl は脆弱ではありません。OpenSSL 1.1.1d で修正済み（1.1.1-1.1.1c が影響を受けます）。OpenSSL 1.1.0l で修正済み（1.1.0-1.1.0k が影響を受けます）。OpenSSL 1.0.2t で修正済み（1.0.2-1.0.2s が影響を受けます）。

- CVE-2019-1552：OpenSSL には、TLS での検証に使用する構成ファイルと証明書を見つけることができるディレクトリツリーの内部デフォルトがあります。このディレクトリは OPENSSLDIR と呼ばれ、-\-prefix / -\-openssldir 設定オプションで設定できます。OpenSSL バージョン 1.1.0 および 1.1.1 の場合、mingw 構成のターゲットは、結果として得られるプログラムとライブラリが UNIX のような環境にインストールされること、およびプログラムのインストール先と OPENSSLDIR のデフォルトのプレフィックスが「/usr/local」であることを前提としています。ただし、mingw プログラムは Windows プログラムであるため、それらのプログラム自体は「C:/usr/local」のサブディレクトリを検索します。このディレクトリはグローバルに書き込み可能な場合があります。そのため、信頼できないユーザーが OpenSSL のデフォルト設定を変更したり、CA 証明書を挿入したりすることがあり得ます。OpenSSL 1.0.2 の場合、「/usr/local/ssl」は、Visual C ビルドを含むすべての UNIX および Windows ターゲットで OPENSSLDIR のデフォルトとして使用されます。ただし、1.0.2 の多様な Windows ターゲットのうち一部のビルド手順では、独自の -\- プレフィックスを指定するよう勧めています。OpenSSL バージョン 1.1.1、1.1.0、および 1.0.2 は、この問題の影響を受けます。影響を受ける展開の範囲が限られているため、その重大度は低いと評価されており、現時点では新しいリリースは作成されていません。OpenSSL 1.1.1d で修正済み（1.1.1-1.1.1c が影響を受けます）。OpenSSL 1.1.0l で修正済み（1.1.0-1.1.0k が影響を受けます）。OpenSSL 1.0.2t で修正済み（1.0.2-1.0.2s が影響を受けます）。
- CVE-2019-1563：攻撃者が復号対象として非常に多くのメッセージを送信した後、復号の試行の成功または失敗の自動通知を受信した場合、攻撃者は CMS/PKCS7 で転送された暗号化キーを回復することや、Bleichenbacher パディングオラクル攻撃を使用して、公開 RSA キーで暗号化された RSA 暗号化メッセージを復号できることがあります。アプリケーションが CMS_decrypt または PKCS7_decrypt 関数に対して秘密 RSA キーとともに証明書を使用して、復号化する正しい受信者情報を選択した場合には、アプリケーションは影響を受けません。OpenSSL 1.1.1d で修正済み（1.1.1-1.1.1c が影響を受けます）。OpenSSL 1.1.0l で修正済み（1.1.0-1.1.0k が影響を受けます）。OpenSSL 1.0.2t で修正済み（1.0.2-1.0.2s が影響を受けます）。
- CVE-2020-1968：Raccoo 攻撃は、TLS 仕様の欠陥を悪用し、攻撃者が Diffie-Hellman（DH）ベースの暗号スイートを使用した接続でプレマスターシークレットを計算できるようにします。このような場合、攻撃者がは、その TLS 接続で送信されるすべての暗号化通信を傍受できることになります。この攻撃は、実装が複数の TLS 接続で DH シークレットを再利用している場合にのみエクスプロイトできます。この問題は DH 暗号スイートにのみ影響し、楕円曲線 DH 暗号スイートには影響しません。この問題は、サポート対象外であり、公開されている更新を受信しなくなった OpenSSL 1.0.2 に影響します。OpenSSL 1.1.1 はこの問題に対して脆弱ではありません。OpenSSL 1.0.2w で修正済み（1.0.2-1.0.2v が影響を受けます）。
- CVE-2021-23840：EVP_CipherUpdate、EVP_EncryptUpdate、および EVP_DecryptUpdate への呼び出しは、入力長がプラットフォームの整数の最大許容長に近い場合に、出力長引数をオーバーフローする場合があります。この場合、関数コールの戻り値は 1 (成功を示す) ですが、出力長の値は負になります。これにより、アプリケーションが正しく動作しなかったり、クラッシュしたりする可能性があります。OpenSSL バージョン 1.1.1i 以前は、この問題の影響を受けます。これらのバージョンのユーザは、OpenSSL 1.1.1j にアップグレードする必要があります。OpenSSL バージョン 1.0.2x 以前は、この問題の影響を受けます。ただし、OpenSSL 1.0.2 はサポート対象外であり、公開されて

© 2025 Cisco and/or its affiliates. All rights reserved.

いる更新は受信されなくなりました。OpenSSL 1.0.2 のプレミアムサポートのお客様は、1.0.2y にアップグレードする必要があります。他のユーザーは 1.1.1j にアップグレードする必要があります。OpenSSL 1.1.1j で修正済み（1.1.1-1.1.1i が影響を受けます）。OpenSSL 1.0.2y で修正済み（1.0.2-1.0.2x が影響を受けます）。

- CVE-2021-3711：SM2 暗号化データを暗号解読するために、アプリケーションは API 関数 EVP_PKEY_decrypt() を呼び出す必要があります。通常、アプリケーションはこの関数を 2 回呼び出します。最初の開始時には、「out」パラメーターを NULL にすることができ、終了時には、暗号解読された平文を保持するために必要なバッファサイズが「outlen」パラメーターに設定されます。その後、アプリケーションは十分なサイズのバッファを割り当てた上で、EVP_PKEY_decrypt() を再度呼び出すことができます。SM2 暗号解読コードの実装のバグとしては、EVP_PKEY_decrypt() への最初の呼び出しによって返されるプレーンテキストを保持するために必要なバッファサイズの計算が、2 番目の呼び出しによって必要とされる実際のサイズよりも小さくなっていることが原因である場合があります。これにより、アプリケーションによって EVP_PKEY_decrypt() が小さすぎるバッファを使用して 2 回目に呼び出されたときに、バッファオーバーフローが発生する可能性があります。暗号解読のために SM2 コンテンツをアプリケーションに提示できる攻撃者は、攻撃者が選択したデータを最大 62 バイトまでバッファからオーバーフローさせ、バッファの後に保持されている他のデータの内容を変更することがあります。バッファの場所はアプリケーションによって異なりますが、通常はヒープが割り当てられます。OpenSSL 1.1.1l （影響を受ける 1.1.1-1.1.1k）で修正されました。
- CVE-2021-3712 –ASN.1 文字列は、OpenSSL では内部的に ASN1_STRING 構造として表されます。これには、文字列データを保持するバッファと、バッファ長を保持するフィールドが含まれます。これは、NUL (0) バイトで終了する文字列データのバッファとして表される通常の C 言語文字列とは対照的です。厳密な要件ではありませんが、OpenSSL 独自の d2i 関数 (および他の同様の解析関数) を使用して解析される ASN.1 文字列、および ASN1_STRING_set() 関数で値が設定されている文字列は、NUL を追加することにより、ASN1_STRING 構造のバイトアレイを終了します。ただし、アプリケーションは、ASN1_STRING アレイの「データ」および「長さ」フィールドを直接設定することにより、バイトアレイを NUL で終了しない有効な ASN1_STRING 構造を直接構築することができます。これは、ASN1_STRING_set0() 関数を使用して行うこともできます。ASN.1 データを出力する多数の OpenSSL 関数は、ASN1_STRING バイトアレイが NUL で終了することを想定していますが、これは直接構築された文字列に対しては保証されていません。アプリケーションが ASN.1 構造の印字を要求し、その ASN.1 構造に、データフィールドを NUL で終了させることなくアプリケーションによって直接構築された ASN1_STRING が含まれている場合、読み取りバッファオーバーランが発生する可能性があります。同じことが、証明書の名前制約処理中にも発生する可能性があります (たとえば、証明書が OpenSSL 解析関数を介してロードする代わりにアプリケーションによって直接構築され、証明書に NUL で終了しない ASN1_STRING 構造が含まれている場合)。X509_get1_email()、X509_REQ_get1_email()、および X509_get1_ocsp() 関数でも発生する可能性があります。攻撃者は、アプリケーションに ASN1_STRING を直接構築させ、影響を受ける OpenSSL 関数の 1 つを介してそれを処理させて、この問題を生じさせる可能性があります。これにより、クラッシュが発生する可能性があります（サービス拒否攻撃を引き起こします）。また、プライベートメモリの内容（プライベートキー、機密性の高い平文など）が漏洩する可能性もあります。OpenSSL 1.1.1l （影響を受ける 1.1.1-1.1.1k）で修正されました。OpenSSL 1.0.2za で修正済み（1.0.2-1.0.2y が影響を受けます）。
- CVE-2022-0778：モジュラ平方根を計算する BN_mod_sqrt() 関数に、非素数モジュライに対して永久にループする可能性のあるバグが含まれています。この関数は内部的に、圧縮形式の楕円曲線公開キー、または圧縮形式でエンコードされたベースポイントを持つ明示的な楕円曲線パラメータを含む証明書を解析するときに使用されます。無効かつ明示的な曲線パラメータを持つ証明書を作成することで、無限ループをトリガできます。証明書の解析は証明書の署名の検証前に行われるため、外部から提供された証明書を解析するプロセスは、サービス拒否攻撃の対象となる可能性があります。明示

© 2025 Cisco and/or its affiliates. All rights reserved.

的な楕円曲線パラメータが含まれている可能性があるため、細工された秘密キーを解析するときにも無限ループに到達する可能性があります。したがって、サーバー証明書を使用する TLS クライアント、クライアント証明書を使用する TLS サーバー、顧客から証明書または秘密キーを取得するホスティングプロバイダー、加入者からの認証要求を解析する認証局、および ASN.1 の楕円曲線パラメータを解析するその他のアプリケーションは脆弱であり、また、攻撃者がパラメータ値を制御できる BN_mod_squart() を使用するモジュールは、この DoS の問題に対して脆弱です。OpenSSL 1.0.2 バージョンでは、証明書の最初の解析中に公開キーが解析されないため、無限ループをトリガするのが少し難しくなります。ただし、証明書の公開キーを必要とする操作は、無限ループをトリガします。特に、攻撃者は自己署名証明書を使用して、証明書署名の検証中にループをトリガできます。この問題は、OpenSSL バージョン 1.0.2、1.1.1、および 3.0 に影響します。この問題は、2022 年 3 月 15 日のリリース 1.1.1n および 3.0.2 で対処されました。OpenSSL 3.0.2 で修正済み（影響を受ける 3.0.0、3.0.1）。OpenSSL 1.1.1n で修正済み（影響を受ける 1.1.1-1.1.1m）。OpenSSL 1.0.2zd で修正済み（影響を受ける 1.0.2 ~ 1.0.2zc）。

欠陥 ID - CSCwi21161

Cisco UCS サーバーには、次の共通脆弱性識別子（Common Vulnerabilities and 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-2010-4252：1.0.0c より前の OpenSSL で、J-Pake が有効になっている場合、J-Pake プロトコルの公開パラメータが適切に検証されないため、リモートの攻撃者は共有秘密の知識の必要性を回避し、正常にプロトコルの各ラウンドで巧妙に細工された値を送信して認証を実行します。
- CVE-2010-5298：SSL_MODE_RELEASE_BUFFERS が有効になっている場合、1.0.1g を介した OpenSSL の s3_pkt.c の ssl3_read_bytes 関数で競合状態が発生し、リモートの攻撃者がセッション全体でデータをインジェクトしたり、サービス拒否（解放後使用および解析エラー）を促したりします。
- CVE-2011-1945：OpenSSL 1.0.0d 以前の楕円曲線暗号（ECC）サブシステムでは、ECDHE_ECDSA 暗号スイートに楕円曲線デジタル署名アルゴリズム（ECDSA）が使用されている場合、2 進数体上に曲線を適切に実装していません。そのために、コンテキスト依存の攻撃者が、タイミング攻撃とラタイム計算を使用して秘密キーを特定しやすくなります。
- CVE-2011-4108：0.9.8s より前の OpenSSL および 1.0.0f より前の 1.x の DTLS の実装では、特定のパディングが有効な場合にのみ MAC チェックが実行されるため、リモート攻撃者はパディングオラクル攻撃によってプレーンテキストを容易に回復できます。
- CVE-2011-4576：OpenSSL 0.9.8s および 1.0.0f より前の 1.x での SSL 3.0 の実装では、ブロック暗号パディングのデータ構造が適切に初期化されないため、リモートの攻撃者が SSL ピアによって、送信されたパディングデータを復号して機密情報を取得する可能性があります。
- CVE-2011-4577：RFC 3779 のサポートが有効になっている場合、0.9.8s より前の OpenSSL および 1.0.0f より前の 1.x で、リモートの攻撃者は、サービス拒否（アサーションの失敗）を生じさせることができます。これは、X.509 証明書が、（1）IP アドレスブロックまたは（2）自律システム（AS）識別子と関連付けられた証明書拡張子データを含んでいることによります。
- CVE-2011-4619：0.9.8s より前の OpenSSL および 1.0.0f より前の 1.x のサーバーゲートウェイ暗号化（SGC）の実装では、ハンドシェイクの再起動が適切に処理されません。これにより、リモート攻撃者は、未指定のベクトルによってサービス拒否（CPU 消費）を生じさせることができます。
- CVE-2012-0027：1.0.0f より前の OpenSSL の GOST エンジンは、GOST ブロック暗号の無効なパラメータを適切に処理しないため、リモートの攻撃者が TLS クライアントから細工されたデータを利用して、サービス拒否（デーモンクラッシュ）を引き起こす可能性があります。
- CVE-2013-6449：1.0.2 より前の OpenSSL の ssl/s3_lib.c の ssl_get_algorithm2 機能が、誤ったデータ構造から特定のバージョン番号を取得する。これにより、リモート攻撃者は、TLS 1.2 クライア

© 2025 Cisco and/or its affiliates. All rights reserved.

ントから取り出して加工されたトラフィックにより、サービス拒否（デーモンクラッシュ）を生じさせることがあります。

- CVE-2014-0076：1.0.0l による OpenSSL の Montegomery 段階の実装では、特定のスワップ操作に一定時間動作が確保されません。これにより、ローカルユーザーが FLUSH + RELOAD キャッシュサイドチャネル攻撃を介して ECDSA ナンスを取得しやすくなります。
- CVE-2014-3566：SSL プロトコル 3.0 は、1.0.1i および他の製品を介して OpenSSL で使用されているように、非決定性 CBC パディングを使用します。これにより、中間者攻撃者がパディングオラクル攻撃を介してクリアテキストデータを取得しやすくなります。これは、別名「POODLE」問題とも呼ばれます。
- CVE-2014-3567：0.9.8zc より前の OpenSSL、1.0.0o より前の 、および 1.0.1 より前の 1.0.1j の t1_lib.c の tls_decrypt_ticket 関数ではメモリリークが発生します。そのため、リモート攻撃者は、完全性チェックの失敗をトリガーするように細工されたセッションチケットを介して、サービス妨害（メモリ消費）が行えます。
- CVE-2014-3568：0.9.8zc より前の OpenSSL、1.0.0o より前の 1.0.0、および 1.0.1j より前の 1.0.1 では、no-ssl3 ビルドオプションが適切に適用されません。これにより、リモート攻撃者は、s23_clnt.c および s23_srvr.c に関連する SSL 3.0 ハンドシェイクで、意図されているアクセス制限をバイパスできます。
- CVE-2014-3570：0.9.8zd より前の OpenSSL、1.0.0p より前の 1.0.0、および 1.0.1k より前の 1.0.1 での BN_scr の実装で、BIGNUM 値の 2 乗が正しく計算されないため、リモート攻撃者が、crypto/bn/asm/mips.pl、crypto/bn/asm/x86_64-gcc.c、および crypto/bn/bn_asm.c に関連する未指定のベクトルを介して、暗号保護メカニズムを突破することが容易になります。
- CVE-2014-3571：0.9.8zd より前の OpenSSL、1.0.0p より前の 1.0.0、および 1.0.1k より前の 1.0.1 で、リモート攻撃者が細工された DTLS メッセージを介してサービス妨害（NULL ポインタの逆参照とアプリケーションのクラッシュ）を引き起こすことが可能になります。これは、d1_pkt.c の dtls1_get_record 関数と s3_pkt.c の ssl3_read_n 関数に関連して、ハンドシェイクヘッダーに対する読み取り操作が、ハンドシェイク本文とは異なる読み取り操作で処理されるためです。
- CVE-2014-3572：0.9.8zd より前の OpenSSL、1.0.0p より前の 1.0.0、および 1.0.1k より前の s3_clnt.c では、ssl3_get_key_exchange 関数により、リモート SSL サーバーが ECDHE から ECDH へのダウングレード攻撃を実行でき、ServerKeyExchange メッセージを省略して転送秘密の損失がトリガーされます。
- CVE-2014-8275：0.9.8zd より前の OpenSSL、1.0.0p より前の 1.0.0、および 1.0.1k より前の 1.0.1 では、証明書データに特定の制約が適用されず、リモート攻撃者は、証明書の未署名部分内に細工されたデータを含めることによって、フィンガープリントベースの証明書ブラックリストを突破することが可能です。これは、crypto/asn1/a_verify.c、crypto/dsa/dsa_asn1.c、crypto/ecdsa/ecs_vrf.c、および crypto/x509/x_all.c に関連しています。
- CVE-2015-0204：0.9.8zd より前の OpenSSL、1.0.0p より前の 1.0.0、および 1.0.1k より前の s3_clnt.c の ssl3_get_key_exchange 関数により、リモート SSL サーバーは、RSA-to-EXPORT_RSA ダウングレード攻撃を実行できます。「FREAK」の問題に関連して、非準拠のロールで脆弱なエフェメラル RSA キーを提供することにより、ブルートフォース復号を容易にします。注：この CVE の範囲は、OpenSSL に基づくクライアントコードのみであり、サーバーまたはその他の TLS 実装に関連する EXPORT_RSA の問題ではありません。
- CVE-2015-0209：0.9.8zf より前の OpenSSL、1.0.0r より前の 1.0.0、1.0.1m より前、および 1.0.2 1.0.2a より前では、リモートの攻撃者が、インポート時に不適切に処理される不正な楕円曲線（EC）秘密キーファイルにより、リモートの攻撃者によってサービス妨害（メモリの破損やアプリケ

© 2025 Cisco and/or its affiliates. All rights reserved.

ーションのクラッシュ）を引き起こされたり、その他、特定されない他の影響が生じる可能性があります。

- CVE-2015-0286：0.9.8zf より前の OpenSSL、1.0.0r より前の 1.0.0、1.0.1 より前、および 1.0.2a より前の 1.0.2 では、OpenSSL の crypto/asn1/a_type.c の ASN1_TYPE_cmp 関数は機能しません。ブール型の比較を適切に実行することで、リモートの攻撃者が、証明書検証機能を使用するエンドポイントに対して、細工された X.509 証明書を利用して、サービス拒否（無効な読み取り操作やアプリケーションのクラッシュ）を引き起こすことが可能になります。
- CVE-2015-0287：0.9.8zf より前の OpenSSL、1.0.0r より前、1.0.0、1.0.1m より前、および 1.0.2a より前の OpenSSL の crypto/asn1/tasn_dec.c の ASN1_item_ex_d2i 関数は、CHOICE および ADB データ構造を再初期化しません。そのため、攻撃者は ASN.1 構造の再利用に依存するアプリケーションを利用して、サービス拒否（無効な書き込み操作およびメモリ破損）を引き起こす可能性があります。
- CVE-2015-0288：0.9.8zf より前の OpenSSL、1.0.0r より前の 1.0.0、1.0.1m より前、および 1.0.2a より前の OpenSSL の crypto/x509/x509_req.c の X509_to_X509_REQ 関数は、許可する場合があります。攻撃者が、無効な証明書キーを介してサービス妨害（NULL ポインタの逆参照とアプリケーションのクラッシュ）を引き起こします。
- CVE-2015-0289：0.9.8zf より前の OpenSSL、1.0.0r より前の 1.0.0、1.0.1m より前の 1.0.1、および 1.0.2a より前の 1.0.2 での PKCS#7 実装は、外部のコンテンツ情報の欠如を適切に処理しません。攻撃者は、任意の PKCS#7 データを処理するアプリケーションを利用し、crypto/pkcs7/pk7_doit.c および crypto/pkcs7/pk7_lib.c に関連した不正なデータを ASN.1 エンコードに提供します。
- CVE-2015-0293：0.9.8zf より前の OpenSSL、1.0.0 より前の 1.0.0r、1.0.1 より前の 1.0.1m、および 1.0.2 より前の 1.0.2a での SSLv2 実装では、リモートの攻撃者が、細工された CLIENT-MASTER-KEY メッセージを通して、サービス拒否（ s2_lib.c アサーションの失敗とデーモンの終了）を可能にします。
- CVE-2015-1788：0.9.8s より前の OpenSSL、1.0.0e より前の 1.0.0、1.0.1n より前の 1.0.1、および 1.0.2b より前の 1.0.2 では、OpenSSL の crypto/bn/bn_gf2m.c の BN_GF2m_mod_inv 関数は機能せず、曲線が不正な形式のバイナリ多項式フィールドを越える ECParameters 構造を適切に処理しません。これにより、リモートの攻撃者は、サポート対象のクライアント認証を行うサーバーに対する攻撃で示されているように、楕円曲線アルゴリズムを使用するセッション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-2015-1789：0.9.8zg より前の OpenSSL、1.0.0s より前の 1.0.0、1.0.1n より前、および 1.0.2b より前の OpenSSL の crypto/x509/x509_vfy.c の X509_cmp_time 関数は、リモートを許可します。カスタム検証コールバックによるクライアント認証をサポートするサーバーに対する攻撃で示されるように、攻撃者は ASN1_TIME データ内の細工された長さフィールドを介して、サービス妨害（境界外読み取りおよびアプリケーションのクラッシュ）を引き起こします。
- CVE-2015-1790：0.9.8zg より前の OpenSSL、1.0.0s より前の 1.0.0、1.0.1n より前、および 1.0.2 b より前の OpenSSL の crypto/pkcs7/pk7_doit.c の PKCS7_dataDecode 関数は、リモート攻撃者を許可します。ASN.1 エンコーディングを使用し、内部の EncryptedContent データが存在しない PKCS#7 BLOB を介してサービス妨害 (NULL ポインタの逆参照およびアプリケーションのクラッシュ) を発生させます。
- CVE-2015-1791：0.9.8zg より前の OpenSSL、1.0.0s より前、1.0.1、1.0.2b より前、1.0.2 マルチスレッドクライアントで使用された場合、リモートの攻撃者が、以前に取得したチケットを再利用しようとしているときに NewSessionTicket を提供することにより、サービス拒否（二重解放およびアプリケーションクラッシュ）を引き起こしたり、その他の影響を与えたりする可能性があります。

© 2025 Cisco and/or its affiliates. All rights reserved.

- CVE-2015-1792：0.9.8zg より前の OpenSSL、1.0.0s より前、1.0.1、1.0.1n より前、および 1.0.2b より前の OpenSSL の crypto/cms/cms_smime.c の do_free_upto 関数で、リモート n の o 攻撃者は、ハッシュ機能の認識できない X.660 OID で示されるように、BIO データ構造の NULL 値をトリガーするベクトルを介してサービス妨害（無限ループ）を引き起こします。
- CVE-2015-3195：0.9.8zh より前の OpenSSL、1.0.0t より前の 1.0.0、1.0.1q より前の 1.0.1、および 1.0.2e より前の 1.0.2 で、OpenSSL の crypto/asn1/tasn_dec.c に ASN1_TFLG_COMBINE を実装すると、エラーが誤処理される不正な形式の X509_ATTRIBUTE データが原因で、リモートの攻撃者は、PKCS#7 または CMS アプリケーションでの復号化の失敗をトリガーして、プロセスメモリから機密情報を取得できます。
- CVE-2015-4000：TLS プロトコル 1.2 以前では、DHE_EXPORT 暗号スイートがサーバーで有効になっていて、クライアントでは有効になっていない場合、DHE_EXPORT の選択が正しく伝達されません。これにより、中間者攻撃者は暗号を実行できます。たとえば、ダウングレード攻撃、つまり ClientHello を DHE に置き換えて、DHE を DHE に書き換えてから、ServerHello を DHE に置き換えて、DHE_EXPORT に書き換えることで攻撃します。これは「Logjam」の問題です。
- CVE-2016-0703：0.9.8zf より前の OpenSSL、1.0.0r より前の 1.0.0、1.0.1m より前、および 1.0.2a より前の OpenSSL での SSLv2 実装の s2_srvr.c の get_client_master_key 関数が、ゼロ以外の CLIENT-MASTER-KEY CLEAR-KEY-LENGTH 値を任意の暗号に使用できます。これにより、中間者攻撃者は、MASTER-KEY 値を特定し、CVE-2016-0800 に関連する問題である Bleichenbacher RSA パディングオラクルを利用して TLS 暗号文データを復号できます。
- CVE-2016-0704：0.9.8zf より前の OpenSSL、1.0.0r より前の 1.0.0、1.0.1m より前、1.0.2a より前の 1.0.2 では、OpenSSL での s2_srvr.c の get_client_master_key 関数のオラクル保護メカニズムが、エクスポート暗号スイートの使用中に不正な MASTER-KEY バイトで上書きします。これにより、リモートの攻撃者が、CVE-2016-0800 に関連する問題である Bleichenbacher RSA パディングオラクルを利用して TLS 暗号テキストデータを簡単に復号できます。
- CVE-2016-2106：1.0.1t および 1.0.2h より前の OpenSSL では、リモート攻撃者は大量のデータ処理により、crypto/evp/evp_enc.c の EVP_EncryptUpdate 関数で整数オーバーフローを起こさせることができます。
- CVE-2016-2107：1.0.1t および 1.0.2h より前の OpenSSL での AES-NI の実装では、特定のパディングチェック時のメモリ割り当てが考慮されません。これにより、リモート攻撃者はパディングオラクル攻撃を AES CBC セッションに対して行い、機密性の高いクリアテキスト情報を取得できます。注：この脆弱性は、CVE-2013-0169 の誤った修正が原因で存在します。
- CVE-2016-2108：1.0.1o および 1.0.2c より前の OpenSSL の ASN.1 実装により、任意のフィールドでの細工されたシリアル化データを用いて。リモートの攻撃者が任意のコードを実行したり、サービス拒否攻撃（バッファアンダーフローとメモリ破壊）を生じさせたりすることができます。これは「負のゼロ」の問題とも呼ばれます。
- CVE-2016-2109：1.0.1t および 1.0.2h 1.0.2h より前の OpenSSL での ASN.1 BIO 実装の crypto/asn1/a_d2i_fp.c の asn1_d2i_read_bio 関数により、リモートの攻撃者は、短い無効なエンコーディングを介して、サービス妨害（メモリ消費）を引き起こすことが可能になります。
- CVE-2016-2176：1.0.1t および 1.0.2h より前の OpenSSL の crypto/x509/x509_obj.c の X509_NAME_oneline 関数により、細工された EBCDIC ASN.1 データを使用して、リモートの攻撃者がプロセススタックメモリから機密情報を取得したり、サービス攻撃（バッファのオーバーリード）を発生させたりすることが可能になります。
- CVE-2016-7056：OpenSSL 1.0.1u 以前でタイミング攻撃の欠陥が見つかっています。ローカルアクセス権を持つ悪意のあるユーザーが ECDSA P-256 秘密キーを回復できる可能性があります。

© 2025 Cisco and/or its affiliates. All rights reserved.

- CVE-2017-3735：X.509 証明書の IPAddressFamily 拡張の解析中に、1 バイトの上書きが可能です。これにより、証明書の誤ったテキスト表示が発生します。このバグは 2006 年から存在しており、1.0.2m および 1.1.0g より前の OpenSSL のすべてのバージョンに存在します。
- CVE-2021-23840：EVP_CipherUpdate、EVP_EncryptUpdate、および EVP_DecryptUpdate への呼び出しは、入力長がプラットフォームの整数の最大許容長に近い場合に、出力長引数をオーバーフローする場合があります。この場合、関数コールの戻り値は 1 (成功を示す) ですが、出力長の値は負になります。これにより、アプリケーションが正しく動作しなかったり、クラッシュしたりする可能性があります。OpenSSL バージョン 1.1.1i 以前は、この問題の影響を受けます。これらのバージョンのユーザは、OpenSSL 1.1.1j にアップグレードする必要があります。OpenSSL バージョン 1.0.2x 以前は、この問題の影響を受けます。ただし、OpenSSL 1.0.2 はサポート対象外であり、公開されている更新は受信されなくなりました。OpenSSL 1.0.2 のプレミアムサポートのお客様は、1.0.2y にアップグレードする必要があります。他のユーザーは 1.1.1j にアップグレードする必要があります。OpenSSL 1.1.1j で修正済み（1.1.1-1.1.1i が影響を受けます）。OpenSSL 1.0.2y で修正済み（1.0.2-1.0.2x が影響を受けます）。
- CVE-2021-3711：SM2 暗号化データを暗号解読するために、アプリケーションは API 関数 EVP_PKEY_decrypt() を呼び出す必要があります。通常、アプリケーションはこの関数を 2 回呼び出します。最初の開始時には、「out」パラメーターを NULL にすることができ、終了時には、暗号解読された平文を保持するために必要なバッファサイズが「outlen」パラメーターに設定されます。その後、アプリケーションは十分なサイズのバッファを割り当てた上で、EVP_PKEY_decrypt() を再度呼び出すことができます。SM2 暗号解読コードの実装のバグとしては、EVP_PKEY_decrypt() への最初の呼び出しによって返されるプレーンテキストを保持するために必要なバッファサイズの計算が、2 番目の呼び出しによって必要とされる実際のサイズよりも小さくなっていることが原因である場合があります。これにより、アプリケーションによって EVP_PKEY_decrypt() が小さすぎるバッファを使用して 2 回目に呼び出されたときに、バッファオーバーフローが発生する可能性があります。暗号解読のために SM2 コンテンツをアプリケーションに提示できる攻撃者は、攻撃者が選択したデータを最大 62 バイトまでバッファからオーバーフローさせ、バッファの後に保持されている他のデータの内容を変更することがあります。バッファの場所はアプリケーションによって異なりますが、通常はヒープが割り当てられます。OpenSSL 1.1.1l （影響を受ける 1.1.1-1.1.1k）で修正されました。
- CVE-2021-3712 –ASN.1 文字列は、OpenSSL では内部的に ASN1_STRING 構造として表されます。これには、文字列データを保持するバッファと、バッファ長を保持するフィールドが含まれます。これは、NUL (0) バイトで終了する文字列データのバッファとして表される通常の C 言語文字列とは対照的です。厳密な要件ではありませんが、OpenSSL 独自の d2i 関数 (および他の同様の解析関数) を使用して解析される ASN.1 文字列、および ASN1_STRING_set() 関数で値が設定されている文字列は、NUL を追加することにより、ASN1_STRING 構造のバイトアレイを終了します。ただし、アプリケーションは、ASN1_STRING アレイの「データ」および「長さ」フィールドを直接設定することにより、バイトアレイを NUL で終了しない有効な ASN1_STRING 構造を直接構築することができます。これは、ASN1_STRING_set0() 関数を使用して行うこともできます。ASN.1 データを出力する多数の OpenSSL 関数は、ASN1_STRING バイトアレイが NUL で終了することを想定していますが、これは直接構築された文字列に対しては保証されていません。アプリケーションが ASN.1 構造の印字を要求し、その ASN.1 構造に、データフィールドを NUL で終了させることなくアプリケーションによって直接構築された ASN1_STRING が含まれている場合、読み取りバッファオーバーランが発生する可能性があります。同じことが、証明書の名前制約処理中にも発生する可能性があります (たとえば、証明書が OpenSSL 解析関数を介してロードする代わりにアプリケーションによって直接構築され、証明書に NUL で終了しない ASN1_STRING 構造が含まれている場合)。X509_get1_email()、X509_REQ_get1_email()、および X509_get1_ocsp() 関数でも発生する可能性があります。攻撃者は、アプリケーションに ASN1_STRING を直接構築させ、影響を受ける OpenSSL 関数の 1 つを介してそれを処理させて、この問題を生じさせる可能性があります。これにより、クラッシュが発生す

© 2025 Cisco and/or its affiliates. All rights reserved.

る可能性があります（サービス拒否攻撃を引き起こします）。また、プライベートメモリの内容（プライベートキー、機密性の高い平文など）が漏洩する可能性もあります。OpenSSL 1.1.1l （影響を受ける 1.1.1-1.1.1k）で修正されました。OpenSSL 1.0.2za で修正済み（1.0.2-1.0.2y が影響を受けます）。

- CVE-2021-4044：OpenSSL の内部で libssl がクライアント側で X509_verify_cert() を呼び出し、サーバーから提供された証明書を確認します。その関数が負の戻り値を返して、内部エラー（メモリ不足など）を示す場合があります。このような負の戻り値は OpenSSL によって誤って処理されるため、IO 関数（SSL_connect() や SSL_do_handshake() など）は成功を示さず、後続の SSL_get_error() へのコールで SSL_ERROR_WANT_RETRY_VERIFY という値が返されます。この戻り値は、アプリケーションが以前に SSL_CTX_set_cert_verify_callback() を呼び出している場合にのみ、OpenSSL によって返されると想定しています。ほとんどのアプリケーションはこれを行わないため、SSL_ERROR_WANT_RETRY_VERIFY は SSL_get_error() からの SSL_get_error() からの戻り値をまったく予期せず、結果としてアプリケーションが正しく動作しない可能性があります。正確な動作はアプリケーションによって異なりますが、クラッシュ、無限ループ、またはその他の同様の不適切な応答が発生する可能性があります。この問題は、X509_verify_cert() によって証明書チェーンの処理時に内部エラーを示す原因となる OpenSSL 3.0 の別のバグと組み合わせると、より重大になります。これは、証明書にサブジェクト代替名の拡張子が含まれていないが、認証局が名前の制約を適用している場合に発生します。この問題は、有効なチェーンでも発生する可能性があります。2 つの問題を組み合わせることで、攻撃者が誤った、アプリケーション依存の動作を誘導する可能性があります。OpenSSL 3.0.1 で修正済み（3.0.0 が影響を受けます）。

C シリーズ M6 サーバファームウェアリリース 4.3(4.242038) のセキュリティ修正

不具合識別子 ：CSCwk90710

Cisco UCS C シリーズ M6 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ます。

- CVE-2024-24853：一部の Intel(R) プロセッサでのエグゼクティブモニタと SMI 転送モニタ（STM）間の移行の誤った動作順序により、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-2024-24980：一部の第 3 世代、第 4 世代、および第 5 世代の Intel(R) Xeon(R) プロセッサでの保護メカニズムの障害により、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-2024-21829：一部の Intel®プロセッサの UEFI ファームウェアエラーハンドラにおける不適切な入力検証より、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-2024-21781：一部の Intel® プロセッサの UEFI ファームウェアにおける不適切な入力検証により、特権ユーザーがローカルアクセスを通じて情報漏洩やサービス拒否を実行できる可能性があります。
- CVE-2023-43753：Intel® Software Guard Extensions（Intel® SGX）を搭載した一部の Intel® プロセッサの不適切な条件チェックがあると、権限ユーザーがローカルアクセスを介して情報開示を有効にする可能性があります。
- CVE-2024-24968：一部の Intel® プロセッサのハードウェア論理に不適切な有限状態マシン（FSM）があると、権限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-2024-23984：一部の Intel® プロセッサの RAPL インターフェイスに観察可能な不一致があるため、権限ユーザーがローカルアクセスを介して情報開示を有効にする可能性があります。

© 2025 Cisco and/or its affiliates. All rights reserved.

C シリーズ M7 および M6 サーバファームウェアリリース 4.3(4.241063) のセキュリティ修正

不具合識別子 ：CSCwk62266

Cisco UCS C シリーズ M7 および M6 サーバは、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ます。

- CVE-2024-6387：シグナルハンドラに関連する sshd サービスで競合状態が特定されました。LoginGraceTime 期間（デフォルトは 120 秒、以前の OpenSSH バージョンでは 600 秒）内にクライアントが認証に失敗した場合、sshd SIGALRM ハンドラが非同期的にトリガされます。ただし、このハンドラは、syslog() など、シグナルハンドラ内から呼び出すのが安全ではないいくつかの関数を呼び出します。

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。

C シリーズ M5 ファームウェアリリース 4.3(2.240077) のセキュリティ修正

不具合識別子 ：CSCwk62266

Cisco UCS M5 C シリーズ M5 サーバは、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ます。

- CVE-2024-6387：シグナルハンドラに関連する sshd サービスで競合状態が特定されました。LoginGraceTime 期間（デフォルトは 120 秒、以前の OpenSSH バージョンでは 600 秒）内にクライアントが認証に失敗した場合、sshd SIGALRM ハンドラが非同期的にトリガされます。ただし、このハンドラは、syslog() など、シグナルハンドラ内から呼び出すのが安全ではないいくつかの関数を呼び出します。

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。

C シリーズ M5 ファームウェアリリース 4.3(2.240053) のセキュリティ修正

障害 ID：CSCwi59840

Cisco UCS M5 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ます。

- **CVE-2023-48795**：9.6 より前の OpenSSH およびその他の製品で見つかった特定の OpenSSH 拡張機能を備えた SSH トランスポートプロトコルにより、リモートの攻撃者は、一部のパケットが（拡張ネゴシエーションメッセージから）省略されるなどの整合性チェックをバイパスできます。その結果、クライアントおよびサーバでは、一部のセキュリティ機能がダウングレードまたは無効化された接続（Terrapin 攻撃とも呼ばれる）が発生する可能性があります。

これは、これらの拡張機能によって実装された SSH バイナリパケットプロトコル（BPP）が、ハンドシェイクフェーズとシーケンス番号の使用を誤って処理するために発生します。たとえば、SSH による ChaCha20-Poly1305（および Encrypt-then-MAC を使用した CBC）の使用に対する効果的な攻撃がある場合、chacha20-poli1305@openssh.com でバイパスが発生します（CBC が使用されている場合は、-etm @openssh.com MAC アルゴリズム）。

© 2025 Cisco and/or its affiliates. All rights reserved.

C シリーズファームウェアリリース 4.3(2.230270) のセキュリティ修正

障害 ID：CSCwh17053

Cisco UCS C225 および C245 M6 サーバは、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ます。

- CVE-2023-20593：**特定のマイクロアーキテクチャ環境下での Zen 2 CPU の問題により、攻撃者が機密情報にアクセスする可能性があります。**

障害 ID：CSCwh18140

Cisco UCS C125 M5 サーバは、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ます。

- CVE-2023-20593：**特定のマイクロアーキテクチャ環境下での Zen 2 CPU の問題により、攻撃者が機密情報にアクセスする可能性があります。**

C シリーズファームウェアリリース 4.3(2.230207) のセキュリティ修正

不具合 ID：CSCwe96259

Cisco UCS C シリーズ M6 サーバは、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ます。

- CVE-2023-20228：この脆弱性の原因は、ユーザー入力の検証が不十分だったことです。攻撃者は、影響を受けるインターフェースのユーザーに細工されたリンクをクリックさせて、この脆弱性を悪用することができます。エクスプロイトに成功すると、攻撃者はターゲットユーザーのブラウザで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスしたりする可能性があります。

不具合 ID：CSCwf30460

Cisco UCS C シリーズ M6 サーバは、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ます。

- CVE-2022-41804：一部の Intel® Xeon® プロセッサの Intel® SGX または ® TDX での不正なエラーインジェクションにより、特権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-2022-40982：一部の Intel(R) プロセッサの特定のベクトル実行ユニットでの一時的な実行後のマイクロアーキテクチャ状態による情報漏洩により、認証されたユーザーがローカルアクセスを介して情報開示を可能にする可能性があります。**
- CVE-2023-23908：一部の第 3 世代 Intel® Xeon® スケーラブルプロセッサのアクセス制御が不適切なため、特権ユーザーがローカルアクセスを通じて情報漏洩を可能にしてしまう可能性があります。
- CVE-2022-37343：一部の Intel® プロセッサーの BIOS ファームウェアのアクセス制御が不適切なため、特権ユーザーがローカルアクセスを通じて特権の昇格を可能にしてしまう可能性があります。

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID：CSCwf30468

Cisco UCS M5 C シリーズ M5 サーバは、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ます。

- CVE-2022-40982：一部の Intel® プロセッサの特定のベクトル実行ユニットでの一時的な実行後のマイクロアーキテクチャ状態による情報漏洩により、認証されたユーザーがローカルアクセスを介して情報開示を可能にする可能性があります。
- CVE-2022-43505：一部の Intel® プロセッサの BIOS 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通じてサービス拒否を可能にする可能性があります。

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。

注：このソフトウェアリリースには、他のリリースで最初に導入されたバグ修正が含まれている場合があります。詳細を確認するには、バグ ID をクリックして、バグ検索ツールにアクセスします。

表 6 C シリーズ M8 および M7 サーバファームウェアリリース 4.3（6.250044）で解決された問題

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
CSCwb45755	MSTOR-RAID スロット上のストレージコントローラに接続された M.2 SATA ディスクが、Windows Server 2025 のインストール中に検出されません。 影響を受けるストレージコントローラは次のとおりです。 • Cisco UCS C220/C240 M8 サーバー上の UCS-M2-HWRAID2 • Cisco UCS C220/C240 M8 サーバー上の UCSC-M2RM-M8 • Cisco UCS C240 M8 サーバー上の UCSC-M2RR-240M8 これは、上記のストレージコントローラに関する Windows Server 2025 に固有の問題です。 ただし、これらの M.2 ディスクは Windows Server 2022 またはその他のオペレーティングシステムで検出され、完全に機能します。	4.3(6.250039)	4.3(6.250044)

© 2025 Cisco and/or its affiliates. All rights reserved.

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)	4.3(6.250044)
CSCwn51498	Cisco UCS C220 および C240 M8 サーバでは、Windows Server 2025 の起動およびシャットダウン中に、生の OEM SEL レコードが CIMC SEL に記録されます。これはシステムの機能やパフォーマンスには影響しません。	4.3(6.250039)	4.3(6.250044)
CSCwn44614	Cisco UCS C220 および C240 M8 サーバでは、Pre-Boot DMA 保護を有効にすると、HTTP/HTTPS ブート経由で OS ISO イメージをダウンロードするときに速度が低下する可能性があります。この問題は、この設定でブート前のプロセス中に発生します。	4.3(6.250039)	4.3(6.250044)

© 2025 Cisco and/or its affiliates. All rights reserved.

表 7 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 4.3(5.250033) で解決された不具合

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
CSCwo84654	Cisco UCS C225 M8 サーバでは、ライザースロット 1C、1B、または 3C に取り付けられた PCIe Gen5 対応 NIC では、リリース 4.3(5.250030) にアップグレードした後、サポートされている Gen5 ではなくダウングレードされた Gen4 速度の PCIe を使用する場合があります。 これはパフォーマンスに影響しますが、信頼性には影響しません。 ダウングレードされた PCIe リンク速度は、ブート中に BIOS とオペレーティングシステムの両方で表示されます。問題は特定のトリガーなしで発生します。 回避策はありません。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。	4.3(5.250030)		4.3(5.250033)

表 8 X シリーズ M8 5.4（0.250037）および 5.4（0.250035）、M7 5.4（0.250035）、M6 5.4（0.250033）、および B シリーズ M6、M5 5.4（0.250034）サーバファームウェアリリースで解決された問題

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwj61708	Cisco UCS FI ドメインで 160 台のサーバのスケールセットアップと 64K を超える高い PV カウントで複数のサーーのウォームリブートを実行すると、特定の状況でセキュアブートアダプタがすぐに再起動しないことがあります。これは、3 つのシャーシで 22 のブレードの同時ウォームリブートが開始されたスケールセットアップで確認されました。Cisco UCS VIC 15000 シリーズセキュアブートアダプタを搭載した一部のブレードは、ソフトリブート後に SAN からの起動に失敗しました。これらのアダプタは、ファブリックインターコネクトを使用してクリーンアッププロセスを実行し、システムの整合性を維持します。このプロセスは、サーバ BIOS がアダプタを認識する前に終了する必要があります。この問題は、特に FI の非常に高い PV カウントまたは例外的に高い CPU 使用率の条件下で発生します。このような場合、セキュアブートアダプタがクリーンアップを完了する前にサーバ BIOS がブートシーケンスを終了すると、アダプタの検出に失敗する可能性があります。その結果、サーバが SAN から正常に起動しない場合があります。この問題は、Cisco UCS VIC 15000 シリーズアダプタを搭載した Cisco UCS ブレードサーバを使用する構成で発生します。	5.2(2.240053)	5.4(0.250033)
CSCwn52355	Cisco UCS B200-M5 サーバでは、インバンド IP アドレス管理は FI-A と FI-B の間で 30 秒ごとにフェールオーバーし、アプリケーションセントリックインフラストラクチャ（ACI）に影響を与えます。アウトオブバンド IP アドレスを使用するか、システムをリセットすることで解決できます。	5.1(0.230075)	5.4(0.250034)

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwj60167	Cisco UCS B シリーズサーバでは、「ハングタスクまたは Oops」が原因でカーネルパニックから BMC が再起動することがあり、管理プレーンにのみ影響します。データプレーンは引き続き機能しますが、ブレードは一時的に管理できなくなります。障害コード F1681 は CIMC 接続損失を示します。ウォッチドッグリセットを示す SEL ログで確認できます。ブレードは、予期しない BMC の再起動後に自動的に回復します。	5.2(2.240053) 5.2(0.230100) 4.2(3j)	5.4(0.250034) 5.3(0.250021)
CSCwk71382	一部のサーバは、デバイスコネクタの更新後に Intersight から切断され、オンラインのままですがアクセスできません。これは、複数のデバイスコネクタバージョンに影響しますが、既知のバグはありません。お客様は、FI コンソールから技術サポートバンドルを生成するか、サーバを再装着することで、問題を解決できます。	5.2(0.230092) 5.2(0.230040)	5.4(0.250033) 5.4(0.250034)
CSCwn28051	Intersight 管理モードの Cisco UCS X210c M6 サーバは、次のアラートを表示します。「Intel PCH Secure Fuse 検証がマザーボードで失敗しました（Intel PCH Secure Fuse Verification has failed on Motherboard）」。サーバは正常に機能し、アラートは通常 CIMC または CMOS をリセットすることでクリアできます。	5.2(2.240053)	5.4(0.250033)
CSCwo05709	Intersight 管理モード（IMM）は、プライベート仮想アプライアンス（PVA）、接続済み仮想アプライアンス（CVA）、またはソフトウェアを使用しているかどうかにかかわらず、Cisco UCS B200 M5、M6、および X210c M6、M7 サーバでのマスク不可能割り込み（NMI）診断をサポートしていません。as a Service（SaaS）モデル。NMI 診断は、OS フリーズを解決するために重要です。 この修正は機能強化されています。	–	5.4(0.250033) 5.4(0.250034) 5.4(0.250035)

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwo15215	Intersight に接続されている Cisco UCS X210c M6 サーバは、DC および CIMC が引き続き実行されていても切断状態のままになる場合があります。ユーザーには、「X 時間または数日前にサーバへの接続が失われました。この時点では、データは関連していない可能性があります。ターゲットの詳細を表示します。」この切断にもかかわらず、CIMC は動作を維持し、接続とコマンドの実行は可能です。管理性を復元するための再起動またはサーバスロットのリセットについては、テクニカルサポートセンターにお問い合わせください。	5.4(0.250011)	5.4(0.250033)
CSCwo40461	Cisco UCS X210c M7 サーバは、Cisco 統合管理コントローラ（CIMC）のメモリ不足（OOM）状態が原因で、シャローディスカバリの問題が発生します。CIMC は OOM 後自動的に回復し、検出プロセスを完了できるようになります。ログは、BMC ファームウェアバージョン 5.2（0.230041）を搭載した UCSX-210C-M7 ハードウェアでの OOM 状態による CIMC リセットを確認しますが、問題はこのバージョンに限定されません。	5.2(0.230041)	5.4(0.250035)

表 9 C シリーズ M8 ファームウェアリリース 4.3(6.250040) および 4.3(6.250039) で解決された問題

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
CSCwn48372	Cisco UCS M8 サーバでは、CbsCmnEfficiencyModeEnRs の BIOS トークンを Auto に設定すると、値がハイパフォーマンスモードとして誤って表示されます。この問題は表示のみに影響し、機能への影響はありません。Intersight は値を [自動（Auto）] として送信し、BMC はデフォルトのパフォーマンスモードを正しく設定します。	4.3(5.240021)	4.3(6.250040)

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwo60509	Cisco UCS C240 M8 サーバで、コントローラが No Raid システムに接続されており、U.3 NVMe ドライブがコントローラの下で使用されている場合は、バックプレーンのデフォルトへのリセットを実行するか、バックプレーン管理をコントローラ接続に手動で変更します。	4.3(6.250026)	4.3(6.250039)

表 10 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 4.3(5.250030) で解決された不具合

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
CSCwk33013	Cisco UCS M5 サーバで EFI セキュアブートキーエラー [0x5304] が発生しています。この問題は、セキュアブートキー（DB、DBx、PK、KEK）がゼロファイルサイズに設定されている場合に発生します。	4.3(2.240090)	4.3(5.250030)
CSCwm67863	RHEL 9.4 を実行している Cisco UCS サーバで、BIOS をアップグレードし、ブートモードを非セキュアからセキュアに切り替えると、ホストの電源がオフになります。	4.3(5.250001)	4.3(5.250030)
CSCwn48372	Cisco UCS M8 サーバでは、CbsCmnEfficiencyModeEnRs の BIOS トークンを「Auto」に設定すると、値がハイパフォーマンスモードとして表示されます。	4.3(5.240021)	4.3(5.250030)
CSCwn85649	イーサネット網アダプタ I710 は、i40e ドライバを利用して、「i40e 0000:17:00.0: ARQ: Unknown event 0x0000 ignored」というメッセージを繰り返し表示します。	4.3(4.240152)	4.3(5.250030)
CSCwn62845	Cisco UCS C220 M7 サーバは、ストレージ RAID バッテリ MRAID の低下を報告し、バッテリまたはコントローラの問題を示しています。	4.3(4.242038)	4.3(5.250030)

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwn65087	サーバファームウェアを 4.3(2.240090) にアップグレードすると、IP フィルタリングエントリが 3 つを超えると、HTTP/ HTTPS アクセスが失われます。HTTP/ HTTPS を手動で再度有効にして、アクセスを復元します。	4.3(2.240090)	4.3(5.250030)

表 11 C シリーズ M5 サーバファームウェアリリース 4.3(2.250021) による解決済みの問題

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
CSCwn97854	4.3(2.240107) から 4.3(2.250016) にアップグレードする場合、Cisco UCS C240 M5 サーバーでのサーバープロファイルのアクティブ化が失敗します。	4.3(2.250016)	4.3(2.250021)

表 12 X シリーズ M8、M7、M6 5.3(0.250021) および B シリーズ M6、M5 5.3(0.250021) サーバファームウェアリリースで解決された不具合

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
CSCwj60167	UCS -B サーバは、管理プレーンにのみ影響を与える「ハングタスクまたは Oops」が原因でカーネルパニックから BMC の再起動が発生する可能性があります。データプレーンは引き続き機能しますが、ブレードは一時的に管理できなくなります。障害コード F1681 は CIMC 接続損失を示します。ウォッチドッグリセットを示す SEL ログで確認できます。	4.3(2c)	5.3(0.250021)
CSCwm13829	UCSX-X10C-RAIDF RAID コントローラを搭載した Cisco UCS X210c M6 または M7 サーバでは、BBU 障害が発生し、そのことがログの安全ステータス登録 0xf000 によって示される場合があります。これは、電圧測定値が異常であることを示し、BBU が不良で、交換が必要な可能性があることを推奨します。解決するには、起動中に RAID セットアップにアクセスし、工場出荷時のデフォルトにリセットして、変更を確認し、保存します。	5.2(0.230092)	5.3(0.250021) 5.0（4i）

© 2025 Cisco and/or its affiliates. All rights reserved.

表 13 X シリーズ M8、M7、M6 および B シリーズ M6、M5 サーバファームウェアリリースで解決された不具合

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
CSCwm72893	まれに、組み込み CPU（eCPU）のソフトウェア異常が原因で Cisco UCS VIC アダプタでファームウェアのハングが発生し、ウォッチドッグタイムアウトとマスク不可能割り込み（NMI）が発生することがあります。これにより、一時的にストレージ接続が失われる可能性があります。最新のファームウェアアップデートでは、このような発生を防ぐためにエラー処理メカニズムを強化することにより、この問題に対処しています。	4.2(3i)	5.3(0.250001)
CSCwm36266	特定の状況では、ウォッチドッグリセットまたはカーネルパニック後、ブレード IOM がブレードを誤ってセーフモードに設定し、ファンがフルスピードで回転する可能性があります。 この問題は、CIMC カーネルでパニックが発生し、リブートが完了する前に、IOM が CIMC 機能を誤って識別し、誤った状態が発生した場合に発生します。この状態は、CIMC またはブレードの再起動後も維持され、ファン速度は上昇します。問題は Cisco UCS B200 M6 ブレードサーバーで確認されています。適切な IOM 通信とブレードの状態管理を確保するために更新が必要です。	4.2(3b)	5.3(0.250001)

表 14 X シリーズ M7 5.2(2.240080) および M6 5.2(2.240078) サーバファームウェアリリースで解決された問題

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
CSCwm26679	サーバーコントローラのドライブ障害が原因でディスクスクラブプロセスが失敗し、次のエラーメッセージが表示されます。 **ディスクスクラブを完了できません** これを解決するには、障害のあるディスクを取り外してから、ディスクのスクラブを再度実行します。	5.2(2.240053)	5.2(2.240080) 5.2(2.240078)

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwm04776	HSU または Redfish 経由で開始されたディスククラブプロセスのタイミングを最適化しました。以前は、このプロセスは完了するまでに約 25 分かかりました。	5.2(2.240053)	5.2(2.240080) 5.2(2.240078)

表 15 X シリーズファームウェアリリース 5.3(0.240016) で解決された不具合

不具合 ID	説明	影響を受ける最初のリリース
CSCwm67631	この問題は、64GB 以上の DIMM がフル装着され、すべてのドライブが取り付けられている、AMD プロセッサを搭載した UCS ブレードサーバーで、以前に電源をオンにしたことがない場合に発生します。 BMC と BIOS を更新した後、[電源オフ（Power Off）] をクリックしてから [CMOS のリセット（Reset CMOS）] をクリックすると、Redfish power-on コマンドを実行した後でも、サーバの電源がオフのままになる障害が発生することがあります。	5.3(99.240008)
CSCwm06766	Cisco UCS X410c M7 の電源が予期せずにオフになり、電源ロックの問題により電源がオンになりません。 Cisco Intersight 経由でサーバーの電源を入れようとすると、次のエラーメッセージが表示されて失敗します。 サーバ電源オンの呼び出し ステータス：失敗 操作がタイムアウトしました。接続/ターゲットエンティティに関連する問題を確認して、再試行してください。	5.2(0.230127)

表 16 X シリーズ M7 サーバファームウェアリリース 5.2(2.240074) による解決済みの問題

不具合 ID	説明	影響を受ける最初のリリース
CSCwk37506	15000 シリーズアダプタを搭載した Cisco UCS サーバーに SAN ブートの複数のパスが設定されていて、1 つのパスに LUN の検出に関する問題があり、別のパスが成功している間に、fnic ドライバが実行するクリーンアップにより、OS のロード時にクラッシュが発生します。この問題は解決されました。	5.2(0.230092)

表 17 X シリーズ M6 および M7 ファームウェアリリース 5.2(2.240053) で解決済みの問題：なし

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明	影響を受ける最初のバンドル
CSCwf13106	Cisco UCS X210c M6 サーバでのファームウェアアップグレードは、Cisco IMC のクラッシュにより停止し、次のメッセージが表示されてプロセスが最大 8 時間遅延します。 **ファームウェアアップグレードの完了を待機します。デバイスへの接続しばらくしてから再度確認してください。** サーバをリセットすると、Cisco IMC との通信が復元され、アップグレードが完了しました。	5.0（1b）
CSCwj07992	8 番目の Cisco UCSX-210C-M7 サーバの検出の問題は、ハードウェア仕様に一致するように最小電力値と最大電力値を変更することで解決されました。	5.1(1.230052)

表 18 X シリーズ M7 ファームウェアリリース 5.2(0.230127) の解決済みの問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwh26280	Cisco UCS X210c M7 サーバで、IPMI ツールがサーバの帯域外（OOB）IP アドレスにクエリを送信した場合、応答を受信するまでに 30 秒以上かかります。この遅延により、予想される応答時間が 30 秒未満のため、モニタリングツールでエラーが表示される原因となります。	5.1(0.230075)

表 19 X シリーズ M7 ファームウェアリリース 5.2(0.230092) の解決済みの問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwh28307	X210cM7 または X410c M7 サーバをバージョン 5.2(0.230041) にアップグレードした後、VIC techsupport ファイルが techsupport パッケージに含まれていませんでした。	5.1(0.230075)

表 20 X シリーズ M7 ファームウェアリリース 5.2(0.230061) の解決済みの問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwh42695	Cisco UCS X410c M7 コンピューティングノードのプラットフォーム ID が、2 つのボードで X210c M7 ID 0x85 ではなく 0x84 として正しく表示されません。	5.2(0.230041)
CSCwd97069	Cisco UCS X410c M7 コンピューティングノードで、PXE ブートポリシーを使用して MK-TME を有効にし、CPU PA 制限を無効にします。OS の起動を試行します。コンピューティングノードが W2K22 および RHEL8.2 で起動できないことが確認されています。	5.2(0.230041)

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明	影響を受ける最初のバンドル
CSCwh10938	Cisco UCS X410c M7 コンピューティングノードには、障害 PLR3 OOB MCC SKU S3 ステッピング修正が必要です。	5.2(0.230041)
CSCwf99117	最適化された電力モードトークンは、Cisco UCS X410c M7 コンピューティングノードで有効になっています。C1E が無効になっていることが確認されます。	5.2(0.230041)

表 21 X シリーズ M6 ファームウェアリリース 5.2(0.230127) の解決済みの問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwi50991	サーバファームウェアバージョン 5.2(0.230040) で動作している Cisco UCS X210c M6 サーバで、ウォッチドッグベースボード管理コントローラ（BMC）で永続的なクラッシュが発生し、サーバの安定性が妨げられるという重大な問題が発生しました。	5.2(0.230040)

表 22 X シリーズ M6 ファームウェアリリース 5.2(0.230040) の解決済みの問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe87623	M6 サーバのすべてのモデルで、電源サイクルごとに、一般的なインベントリ情報の更新に待ち時間が発生し、HCL のステータスが未完了と表示されることが確認されています。GenericInventory mo エントリが削除され、完全に挿入されます。このインベントリ情報の更新中に、OS 情報が欠落していると、OS が起動するまで HCL ステータスが一時的に無効になります。	5.0 (2b)
CSCwf23487	Cisco UCS X シリーズ M6 コンピューティングノードのファームウェアアップグレード後にサーバ検出が失敗します。	5.1(0.230054)

表 23 B シリーズ M6 および M5 サーバファームウェアリリース 5.2(2.240080) で解決された不具合

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwm26679	サーバーコントローラのドライブ障害が原因でディスクスクラブプロセスが失敗し、次のエラーメッセージが表示されます。 **ディスクスクラブを完了できません** これを解決するには、障害のあるディスクを取り外してから、ディスクのスクラブを再度実行します。	5.2(2.240051)	5.2(2.240080)
CSCwm04776	HSU または Redfish 経由で開始されたディスクスクラブプロセスのタイミングを最適化しました。以前は、このプロセスは完了するまでに約 25 分かかりました。	5.2(2.240051)	5.2(2.240080)

表 24 B シリーズファームウェアリリース 5.2(0.230039) で解決された不具合

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe00937	Cisco UCS B200 M6 サーバは SSH 要求に応答しますが、Serial Over LAN（SOL）は無効になっています。hmac-sha1 が SSH に対して有効になっているため、CIMC IP はセキュリティスキャンで脆弱としてフラグが付けられます。	4.2(2d)
CSCwe19822	M5 サーバのすべてのモデルで、カーネルのクラッシュとウォッチドッグのリセットが原因で CIMC のリセットが発生することが確認されています。	4.2(2e)
CSCwe87623	M6 サーバのすべてのモデルで、電源サイクルごとに、一般的なインベントリ情報の更新に待ち時間が発生し、HCL のステータスが未完了と表示されることが確認されています。GenericInventory mo エントリが削除され、完全に挿入されます。このインベントリ情報の更新中に、OS 情報が欠落していると、OS が起動するまで HCL ステータスが一時的に無効になります。	5.1(0.230069)
CSCwf02413	Cisco UCS B200 M6 サーバの場合、関連付けられていないサーバで電力バジェットアラートが表示されます。サーバがサーバプロファイルに関連付けられておらず、検出が成功した場合、アラートは自動的にクリアされます。	4.2(2d)

表 25 C シリーズ M5 サーバファームウェアリリース 4.3(2.240090) による解決済みの問題

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwf93621	Cisco UCS C240 M5SX および UCS HX240c M5SX サーバーで、ファームウェアをリリース 4.2(3d) にアップグレードすると、システムのドライブの障害により検出または関連付けが失敗します。	4.2(3d)	4.3(2.250016) 4.2(3j)
CSCwm45280	Cisco UCS C シリーズサーバーで、Intersight モードでのメモリが少ない Cisco UCS VIC アダプタは、アダプタのインベントリ要求に応答できません。これは、アダプタが要求を処理するプロセスを作成できないためです。	4.2(3b)	4.3(2.250016) 4.3(4.242066) 4.3(2.240107)
CSCwm48655	PSU アラートが Cisco IMC でフラッピングし、SEL ログに PSU エラーメッセージが入力されます。	4.3(3c)	4.3(2.250016)
CSCwn00366	eNIC または vHBA のみが構成されている場合、Intersight 管理モードの Cisco UCS C シリーズサーバーでサーバー検出の障害が発生します。この問題は、palo_vnic_listtype() API コールによってトリガーされた vniccfgd プロセスでのメモリリークが原因で発生します。一定期間にわたってメモリリークが累積されると、最終的に障害につながるしきい値に到達します。	4.3(2.230207)	4.3(2.250016) 4.3(5.250001)
CSCwn56294	Cisco UCS C220 M5 サーバーでは、Cisco IMC が突然再起動し、メモリ不足（OOM）エラーにより BMC がリセットされます。	4.3(2.240053)	4.3(2.250016)
CSCwi95393	ファームウェアバージョン 4.2(3e) を実行し、Intersight CVA バージョン 1.0.9-615 によって管理されている UCSC-C220-M5SX サーバーは、[製品名（Product Name）]、[シリアル番号（Serial Number）]、および CIMC サマリータブの [PID] フィールドにランダムな 32 文字の文字列を表示します。この問題は、CIMC を再起動した後に解決されます。	4.2(3e)	4.3(2.250016) 4.2 (3o)

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwj68672	Cisco UCS 240 M6 サーバーは、ハードウェアプラットフォーム構成の起動プロセス中にスタックし、サーバーはノードのプロファイルを展開またはアクティブ化できません。	4.3(2.230207)	4.3(2.250016)
CSCwm47183	Cisco 12G SAS HBA を搭載した C240-M6L サーバーの Twitter HDD（モデル MG06SCA800A）は、Cohesity によって削除対象としてランダムにマークされます。CIMC ログに障害がないにもかかわらず、Smartctl でマークされるとデータを取得できません。Cohesity ログは、I/O エラーとスーパーブロック読み取りの問題を報告します。JBOD のセットアップに影響しますが、ドライブを再度装着すると、解決する場合があります	4.3(2.240002)	4.3(2.250016) 4.2 (3o) 4.3(5.250001) 4.3(4.242066)

表 26　C シリーズ M8、M7 および M6 4.3(5.250001) サーバファームウェアリリースで解決された不具合

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
CSCwn42969	電源の再投入または Cisco UCS サーバーのリセット後、1.5 週間以上アイドル状態、または最小限のワークロードのままにすると、NVME ディスク FRONT-NVME-2 が動作不能になることがあります。この問題が発生し、ドライブが動作不能の場合は、ドライブの PID と NVME Disk FRONT-NVME の動作不能の問題（CSCwn42969）のドライブ PID を確認します。該当する PID の場合は、Cisco TAC に交換について問い合わせてください。リストに示されていない場合は、ファームウェアリリース 9CV10490 にアップグレードしてください。	4.3(5.240021)	4.3(5.250001) 4.3(4.242066) 4.2(3n)

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwm47183	特定の HDD（モデル MG06SCA800A）に、Cisco IMC ログに障害が示されていなくても、バックアップアプリケーションによる削除マークが予期せず表示されます。この問題は、Cisco 12G SAS HBA コントローラを搭載したファームウェアバージョン 4.3(2.240002) の Cisco UCS C240 M6 サーバーで発生します。 ディスク I/O エラーは、タイムアウトや読み取りの問題を示し、正常なマウントを妨げ、ディスク上のマークの削除につながります。この状況は、バックアップアプリケーションを使用するクラスタに影響し、中断を防ぐためにさらに調査する必要があります。	4.3(2.240002)	4.3(5.250001) 4.3(4.242066) 4.2 (3o) 4.3(2.250016)
CSCwn00366	eNIC または vHBA のみが構成されている場合、Intersight 管理モードの Cisco UCS C シリーズサーバーでサーバー検出の障害が発生します。この問題は、palo_vnic_listtype() API コールによってトリガーされた vniccfgd プロセスでのメモリリークが原因で発生します。一定期間にわたってメモリリークが累積されると、最終的に障害につながるしきい値に到達します。	4.3(2.230207)	4.3(5.250001) 4.3(2.250016)

NVME ディスク FRONT-NVME のドライブ PID の動作不能の問題：CSCwn42969

UCS-NVME4-1600、UCSX-NVME4-1600-D、HX-NVME4-1600、UCS-NVME4-3200、UCSB-NVME4-3200,UCSX-NVME4-3200、HX-NVME4-3200、UCS-NVME4-6400、UCSB-NVME4-6400、UCSX-NVME4-6400、HX-NVME4-6400、UCS-NVME4-1920、UCSB-NVME4-1920、UCSX-NVME4-1920、HX-NVME4-1920、UCS-NVME4-3840、UCSB-NVME4-3840、UCSX-NVME4-3840、HX-NVME4-3840、UCS-NVME4-7680、UCSB-NVME4-7680、UCSX-NVME4-7680、HX-NVME4-7680、UCS-NVME4-15360、UCSB-NVME4-15360、UCSX-NVME4-15360、HX-NVME4-15360、UCSX-NVB1T6O1P、HX-NVB1T6O1PM6、UCS-NVB3T2O1PM6、UCSB-NVA3T2O1P、UCSX-NVB3T2O1PM6、UCS-NVB3T2O1P、UCSX-NVB3T2O1P、HX-NVB3T2O1PM6、UCS-NVB6T4O1PM6、UCSB-NVA6T4O1P、UCSX-NVB6T4O1PM6、UCS-NVB6T4O1P、UCSX-NVB6T4O1P、HX-NVB6T4O1PM6、UCS-NVB1T9O1VM6、UCSB-NVA1T9O1V、UCSX-NVB1T9O1VM6、UCS-NVB1T9O1V、UCSX-NVB1T9O1V、HX-NVB1T9O1VM6、UCS-NVB3T8O1VM6、UCSB-NVA3T8O1V、UCSX-NVB3T8O1VM6、UCS-NVB3T8O1V、UCSX-NVB3T8O1V、HX-NVB3T8O1VM6、UCS-NVB7T6O1VM6、UCSB-NVA7T6O1V、UCSX-NVB7T6O1VM6、UCS-NVB7T6O1V、UCSX-NVB7T6O1V、HX-NVB7T6O1VM6、UCS-NVB15TO1VM6、UCSB-NVA15TO1V、UCSX-NVB15TO1VM6、UCS-NVB15TO1V、UCSX-NVB15TO1V、HX-NVB15TO1VM6

© 2025 Cisco and/or its affiliates. All rights reserved.

表 27 C シリーズ M7 および M6 サーバファームウェアリリース 4.3(4.242066) で解決された不具合

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
CSCwm72893	まれに、ソフトウェアの問題が原因で eCPU がハングすると、Cisco UCS VIC アダプタがハングすることがあります。これにより、一時的なストレージの損失が発生します。	4.2(3i)	4.3(4.242066) 4.3(2.240107)
CSCwm45280	Cisco UCS C シリーズサーバーで、Intersight モードでのメモリが少ない Cisco UCS VIC アダプタは、アダプタのインベントリ要求に応答できません。これは、アダプタが要求を処理するプロセスを作成できないためです。	4.2(3b)	4.3(4.242066) 4.3(2.240107) 4.3(2.250016)
CSCwm02539	複数のサーバーが SAN から ADISC を使用して接続を構築するターゲット（IBM アレイなど）を起動すると、散発的に SAN からの起動が UEFI シェルで失敗することがあります。	4.3.4.240152	4.3(4.242066)
CSCwm58947	Microsoft Windows OS を搭載し、VXLAN、NVGRE、および RDMA で構成された Cisco UCS VIC アダプタを搭載した Cisco UCS サーバーでは、アダプタがハング状態になり、Windows OS で致命的なシステムエラー（BSOD）が発生します。	4.2(3b)	4.3(4.242066)
CSCwn18475	Xen サーバークラスタ内の VIC アダプタがランダムにクラッシュします。エラーが表示され、ネットワークが短時間切断され、タイムアウトが発生します。TAC に問い合わせて支援を求め、必要に応じてサーバーをリブートしてください。	5.2(1.240010)	4.3(4.242066)

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwn42969	Cisco UCS サーバーのリセットまたは電源再投入後、1.5 週間以上アイドル状態になっていた場合、またはワークロードが最小限の場合、NVME ディスク FRONT-NVME-2 が動作を停止することがあります。ドライブが動作不能になった場合、次のように対処してください。 ドライブの製品 ID（PID）が影響を受けるモデルのいずれかであるかどうかを確認します。 該当する PID の場合は、Cisco TAC に交換について問い合わせてください。 該当しない PID の場合は、ファームウェアをバージョン 9CV10490 にアップグレードします。	4.3(5.240021)	4.3(4.242066) 4.2(3n)
CSCwm26679	サーバーコントローラのドライブ障害が原因でディスクスクラブプロセスが失敗し、次のエラーメッセージが表示されます。 ディスクスクラブを完了できません これを解決するには、障害のあるディスクを取り外してから、ディスクのスクラブを再度実行します。	4.3(3.240043)	4.3(4.242066)
CSCwm04776	HSU または Redfish 経由で開始されたディスクスクラブプロセスのタイミングを最適化しました。以前は、このプロセスは完了するまでに約 25 分かかりました。	4.3(3.240043)	4.3(4.242066)

表 28 C シリーズ M5 サーバファームウェアリリース 4.3(2.240107) による解決済みの問題

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
CSCwm72893	まれに、ソフトウェアの問題が原因で eCPU がハングすると、Cisco UCS VIC アダプタがハングすることがあります。これにより、一時的なストレージの損失が発生します。	4.2(3i)	4.3(2.240107) 4.3(4.242066)

© 2025 Cisco and/or its affiliates. All rights reserved.

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
CSCwm45280	Cisco UCS C シリーズサーバーで、Intersight モードでのメモリが少ない Cisco UCS VIC アダプタは、アダプタのインベントリ要求に応答できません。これは、アダプタが要求を処理するプロセスを作成できないためです。	4.2(3b)	4.3(2.240107) 4.3(4.242066) 4.3(2.250016)

表 29 C シリーズサーバファームウェアリリース 4.3(5.240021) で解決された不具合

不具合 ID	説明	影響を受ける最初のリリース
CSCwk73250	Cisco UCS サーバーでは、2 台以上のドライブを使用した RAID 1 構成が OOB ストレージ構成で失敗します。	4.3(5.240094)A
CSCwk87002	Cisco UCS M8 サーバでは、Web UI でホスト名を変更すると、Cisco IMC 証明書がユーザーの同意なしに共通名として新しいホスト名で自動生成されます。	4.3(99.240120)
CSCwk87070	Cisco UCS M8 サーバでは、ダークテーマモードで Web UI を使用しているときに、いくつかのテキストフィールドにラベルが表示されません。そのため、ユーザーはネットワーク関連の操作を実行するためにテキストフィールドを識別できません。	4.3(99.240119)
CSCwk98195	Cisco UCS M8 サーバでは、[マウントオプション（Mount Options）] フィールドのポート番号が Web UI で仮想メディア（vMedia）マッピング用に設定されるように変更されると、仮想メディア（vMedia）は CIFS および NFS 共有の仮想メディア（vMedia）マッピングにデフォルトのポート番号を使用し続けます。	4.3(99.240129)

表 30 C シリーズ M5 サーバファームウェアリリース 4.3(2.240090) による解決済みの問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwm02322	Cisco UCS C220 M5 サーバでは、障害モニタリング用の XML API コマンドはファンアラートをキャプチャしません。 この問題は解決されました。	4.1(3f)
CSCwj86973	Cisco UCS C220 M5 サーバーでは、SNMP ユーザーは **snmpd.conf** SNMP の構成後にファイルに表示されません。	4.2 (2a)

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明	影響を受ける最初のバンドル
CSCwk22654	Cisco UCS C220 M5 サーバーでは、SNMP 応答を改善し、未装着の CPU スロットの応答値を向上させる必要があります。	4.3(2.230270)

表 31 C シリーズ M6 サーバファームウェアリリース 4.3(4.242038) で解決された不具合

不具合 ID	説明	影響を受ける最初のリリース
CSCwk37506	1400 または 15000 シリーズアダプタを搭載した Cisco UCS サーバーに SAN ブートの複数のパスが設定されていて、1 つのパスに LUN の検出で問題があり、別のパスが正常に実行されている場合、OS のロード時に fnic ドライバが行うクリーンアップがクラッシュします。この問題は解決されました。	4.3(3.240043)
CSCwi35681	Cisco UCS C245 M6 サーバーでは、ホスト OS での BIOS アップグレード後、NUMA ノード数がデフォルト値に戻り、構成は保持されません。	4.3(2.240270)
CSCwk70990	Cisco UCS C240 M6 サーバーでは、オンボード LOM コントローラ（x550）を無効にすることはできません。	4.3(2.230270)

表 32 C シリーズ M7 および M6 ファームウェアリリース 4.3(4.241063) で解決された不具合

不具合 ID	説明	影響を受ける最初のリリース
CSCwk45810	Cisco UCS C シリーズ M7 および M6 サーバでは、HSU ISO が CIFS 共有に保存され、リモート CIFS 共有パスワードに次の特殊文字が含まれている場合、HSU Redfish 更新の開始に失敗します。単一引用符（'）、バックスラッシュ（\）、カンマ（,）、または二重引用符（"）。	4.3(2.240053)
CSCwk29026	リリースバージョン 4.3(2.230270) 以降を使用する Cisco UCS C シリーズ M7 および M6 サーバでは、Cisco IMC 構成をインポートすると、LDAP ドメインとドメイングループが入力されません。	4.3(2.230270)
CSCwi52997	Cisco UCS C シリーズ M7 および M6 サーバでは、ネットワークモニタリングツールの使用中または SNMP walk コマンドの実行中に、CIMC のワークロードが低 ~ 中程度の場合、特定の Cisco MIB OID のデータを取得する際に問題が発生する可能性があります。 コマンドは失敗し、次のメッセージが表示されます。 この OID のこのエージェントで使用可能なそのようなオブジェクトはありません。	4.3(4.230064)

© 2025 Cisco and/or its affiliates. All rights reserved.

表 33 C シリーズ M5 ファームウェアリリース 4.3(2.240077) の解決済みの問題：なし

不具合 ID	説明	影響を受ける最初のリリース
CSCwk29026	リリースバージョン 4.3.2.230270 以降を使用する Cisco UCS C シリーズ M5 サーバでは、Cisco IMC 構成をインポートすると、LDAP ドメインとドメイングループが入力されません。 フィールドは、Cisco IMC GUI の以下のタブには入力されません。 **ステップ 1.** [管理者（Admin）] > [ユーザー（Users）] > [LDAP] > [ドメイン（Domain）] **ステップ 2.** [管理者（Admin）] > [ユーザー（Users）] > [LDAP] > [グループ（Groups）] > [ドメイン（Domain）] （指定したグループごと） この問題は解決されました。	4.3(2.230270)

表 34 C シリーズ M5 サーバファームウェアリリース 4.3(2.240053) による解決済みの問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwj09095	ファームウェアバージョン 4.3(2.240002) 以前の Cisco UCS C220 M5SX および C240 M5SX サーバで、XML API を介して SR-IOV プロパティを送信するときにエラーが発生しました。 **XML 解析エラー：要素「adaptorEthSRIOVProfile」** ファームウェアバージョン 4.3(2.240020) 以降にアップグレードすると、この問題が解決されました。	4.3(2.230189)

表 35 C シリーズ M7、M6、および M5 サーバファームウェアリリース 4.3(2.240009) の解決済みの問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwj00617	Cisco UCS C シリーズ M5 および M6 サーバでは、HTTP および TFTP プロトコルを使用した XML API インターフェイスからの SAS エクスパンダファームウェアの更新が失敗し、次のエラーメッセージが表示されます。 **操作に失敗しました。パスワードが無効です。**	4.2(3i)
CSCwi97945	Cisco UCS M5 および M6 サーバでは、HTTP および TFTP プロトコルを使用した Cisco Integrated Management Controller（CLI）インターフェイスからの SAS エクスパンダファームウェアの更新が失敗し、次のエラーメッセージが表示されます。	4.2(3i)

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明	影響を受ける最初のバンドル
	操作に失敗しました。パスワードが無効です。	

表 36 C シリーズファームウェアリリース 4.3(2.240002) で解決された問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwh53073	Cisco UCS C240 M5 SD および Cisco UCS C245 M6 SX では、Cisco Integrated Management Controller（CIMC）から生成されたアラームが Intersight ユーザーインターフェイス（UI）に正確に表示されません。Intersight UI の [アラーム（Alarm）] ページには、イベントの直後にアラームがトリガされたにもかかわらず、関連付けられたアラームの日時が「9 時間後」と表示されていました。	4.2 (2a)
CSCwi04192	Cisco UCS C220 M6 および C240 M6 サーバでは、サードパーティ製の Mellanox MLOM カード（Mellanox UCSC-O-N6CD100GF）は、デフォルトのファンポリシーが適切な冷却を提供できず、ファンの回転数を変更してカードを冷却する必要があるため、過熱状態やリンクのフラップが発生しやすくなります。	4.3(2.230207)

表 37 C シリーズファームウェアリリース 4.3(2.230270) で解決された問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwh34432	Redfish API を使用して vMedia をマウントしているときに、ユーザーが TransferProtocolType フィールドをポストするのを忘れると、次のエラーメッセージが表示されます。 **メッセージ: 不正なリクエスト形式**	4.3(1.230097)
CSCwf44478	Red Hat Enterprise Linux OS バージョン 8.6 and 9.0 を搭載した Cisco UCS C シリーズ M7 サーバで、ホットプラグ後に Micron 7450 NVMe ドライブが検出されません。	4.3(2.230207)
CSCwh13701	Cisco UCS C225 M6 および C245 M6 サーバに電源装置（PSU）が搭載されており、ファームウェアバージョンが 4.2(3h) より前の場合、サーバの電源が警告なしで予期せずにオフになることがあります。	4.3(1.230097)
CSCwf94278	リリースバージョン 4.1(3b)、4.2(2a)、4.2(3b) の Cisco UCS C シリーズ M5 サーバでは、ユーザーは「読み取り専用」ユーザーとのセッションを作成できますが、セッションから削除またはログアウトすることはできず、Redfish API インターフェイスを使用します。	4.2 (2a)

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明	影響を受ける最初のバンドル
CSCwh81377	Cisco UCS C シリーズ M7 サーバで、Intersight を介して仮想メディア（vMedia）ポリシーを展開すると、「既存の仮想メディアの削除エラー：仮想メディア 0、1 がイジェクトされていません。しばらくしてからもう一度お試しください。この問題は、仮想メディア（vMedia）仮想メディア（vMedia）を作成した場合に発生します。	4.3(2.230207)

表 38 C シリーズファームウェアリリース 4.3(2.230207) で解決された問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe19822	M5 サーバのすべてのモデルで、カーネルのクラッシュとウォッチドッグのリセットが原因で CIMC のリセットが発生することが確認されています。	4.2（2f）
CSCwe87623	M6 サーバのすべてのモデルで、電源サイクルごとに、一般的なインベントリ情報の更新に待ち時間が発生し、HCL のステータスが未完了と表示されることが確認されています。GenericInventory mo エントリが削除され、完全に挿入されます。このインベントリ情報の更新中に、OS 情報が欠落していると、OS が起動するまで HCL ステータスが一時的に無効になります。	4.2(3e)

表 39 C シリーズ M7 ファームウェアリリース 4.3（1.230138）で解決された問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe87764	128GB DIMM を搭載した Cisco UCS M7 サーバーでは、システムパフォーマンスを向上させるために電圧レギュレータの値を変更すると、CPU のパフォーマンスが低下する可能性があります。	4.3(1.230124)

表 40 C シリーズ M7 ファームウェアリリース 4.3（1.230124）で解決された問題

不具合 ID	説明	影響を受ける最初のバンドル
CSCwe47118	Redfish monitor core が組み合わせストレス（Redfish stress を含む）中に発生しました。	4.3(1.230097)

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。

注：このソフトウェアリリースには、他のリリースで最初に特定された未解決のバグが含まれている場合があります。詳細を確認するには、バグ ID をクリックして、バグ検索ツールにアクセスします。

© 2025 Cisco and/or its affiliates. All rights reserved.

表 41 X シリーズ M8 5.4（0.250037）および C シリーズ M8 4.3（6.250040）および 4.3（6.250039）、M7、M6 4.3（6.250040）サーバ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ンドル
CSCwo67388	Intersight またはスタンドアロンモードの Cisco UCS X210c M8、C220 M8、および C240 M8 サーバでは、「パスワード履歴」機能が正しく機能しません。[パスワード履歴] フィールドが 1 ~ 5 に設定されている場合、Cisco 統合管理コントローラ (CIMC) では、新しいパスワードを以前のパスワードと照合することができず、パスワードの再利用が可能になります。	繰り返しではない一意のパスワードを使用してください。	4.3(6.250012)
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、アップデート、工場出荷時設定へのリセット、Cisco IMC の再起動、またはその他の操作中にトリガーされた CMOS クリア操作によって BIOS のフラッシュが中断された場合に発生する可能性があります。	次のいずれかを実行します。 1. 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。 2. バックアップ BIOS の Activate。 3. BIOS を更新し、アクティブ化します。	4.3(6.250039)
CSCwe67280	リリースバージョン 4.3.5.250001 の Cisco UCS C シリーズサーバでは、CLI を使用して activate コマンドを実行しても、VIC アウトオブバンド (OOB) ファームウェアアップデートはトリガーされません。	UI または XML インターフェイスを活用か、CLI で「no-activate」オプションを使用します。更新を開始した後、手動でホストの電源を再投入して、更新が正常に完了したことを確認します。	4.3(6.250033)
CSCwn47257	Cisco UCS C シリーズサーバでは、VIC FPGA の変更後に VIC ファームウェアをアップグレードするときに、バージョンの「G」サフィックスで示されるゴールデン FPGA イメージからシステムが起動することがあります。	同じイメージをフラッシュし、ホストの電源再投入を実行します。	4.3(6.250039)

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明	回避策	影響を受ける最初のバンドル
CSCwm33093	U.3/ SAS/SATA ドライブでは、ディスク 1、2、3、および 4 に適用される RAID-10 ストレージプロファイルを作成すると、予期しない動作が発生します。disk-1 を削除するとリモート対応ドライブ（VD）がデグレードされますが、disk-2 を削除すると VD はデグレードされずにオフラインになります。ディスク 1 と 2 を再挿入するとオンライン状態に復元しますが、VD は動作不能のままです。この問題は、ファームウェア主導のスパン割り当てによってユーザー設定がオーバーライドされ、パフォーマンスが最適化されるために発生します。	ファームウェアはパフォーマンスの最適化のために管理ツールの構成をオーバーライドするため、arcconf を活用正確なスパンの割り当てを確認します。	4.3(5.240134)
CSCwo02722	Cisco UCS C240 M7 サーバでは、HUU 4.3.6.250039 以降のリリースと同等のファームウェアバージョン DG02_1.3274-7.0.0.0 にアップグレードすると、UCSC-GPU-FLEX170 のファームウェアアップグレードが失敗します。この問題は、UCSC-GPU-FLEX170 の現在実行中のファームウェアバージョンが DG02_1.3260-6.4.0.0 または DG02_1.3260-6.7.0.0 の場合に発生します。	UCSC-GPU-FLEX170 を中間ファームウェアバージョン DG02_1.3271-6.8.0.0 にアップグレードします。これは、HUU 4.3(4.24xxxx) または 4.3(5.2xxxxx) リリースレベルと同等です。 **注**：言及されている HUU バージョン番号では、「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。	4.3(6.250040)

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明	回避策	影響を受ける最初のバンドル
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、ファームウェアは実際に更新され、バックグラウンドで正常にアクティブ化されます。 **注**：言及されている HUU バージョン番号では、「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)
CSCwo77289	Cisco UCS B シリーズ B200 M5 サーバがファームウェアバージョン 5.3（0.250001）にアップグレードされると、すべての M2 ディスクが温度しきい値を超えの警告を報告します。	以前のファームウェアバージョン 5.3（0.240014）へのロールバック。	5.3(0.250001)
CSCwb45755	ストレージコントローラに接続された M.2 ディスクを搭載した Cisco UCS C220 M8 サーバでは、Windows Server 2025 のインストールページでディスクが検出されません。しかし、Windows Server 2022 のインストール中にディスクが検出されます。これは特に Windows Server 2025 で発生します。	回避策はありません。	4.3(6.250039)
CSCwn99720	2S 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 サーバーでは、Intel SGX は BIOS で有効にした後も無効のままになります。	デュアル CPU 構成を活用します。	4.3(6.250039)

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明	回避策	影響を受ける最初のバンドル
CSCwn51498	Cisco UCS C220 および C240 M8 サーバでは、Windows Server 2025 の起動およびシャットダウン中に、生の OEM SEL レコードが CIMC SEL に記録されます。これはシステムの機能やパフォーマンスには影響しません。	回避策は必要ありません。Windows 2025 の起動中に記録された Raw OEM SEL レコードは無視してください。	4.3(6.250039)

表 42 X シリーズサーバファームウェアリリース 5.3（0.240016）で未解決の問題

不具合 ID	説明	回避策	影響を受ける最初のバンドル
CSCwj96037	RHEL9.3/RHEL9.4 を実行している VM が存在する ESXi 8.0U2 環境で、ホットプラグ可能な Intel® および Micron® NVMe ドライブの取り外しまたは挿入時に問題が発生します。lsblk、lspci、nvme list などのコマンドが正しく更新されないため、誤ったドライブ情報が発生し、VM の電源がオフになる可能性があります。NVMe ドライブの削除または挿入後、VM が新しいドライブの情報を正しく認識および更新しない場合があります。	VM が新しく挿入された NVME ドライブを検出できることを確認するには、次の手順を実行します。 VM の電源をオフにします。 PCIe NVME ドライブを VM 構成に追加します。 VM の電源をオンにします。	5.2(99.241014)

© 2025 Cisco and/or its affiliates. All rights reserved.

表 43 X シリーズ M7 および M6 ファームウェアリリース 5.2(2.240053) 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ンドル
CSCwj61708	Cisco UCS FI ドメインで 160 台のサーバのスケールセットアップと 64K を超える高い PV カウントで複数のサーバのリブートを実行すると、特定の状況でセキュアブートアダプタがすぐに再起動しないことがあります。これは、3 つのシャーシで 22 のブレードの同時ウォームリブートが開始されたスケールセットアップで確認されました。Cisco UCS VIC 15000 シリーズセキュアブートアダプタを搭載した一部のブレードは、ソフトリブート後に SAN からの起動に失敗しました。これらのアダプタは、ファブリックインターコネクトを使用してクリーンアッププロセスを実行し、システムの整合性を維持します。このプロセスは、サーバ BIOS がアダプタを認識する前に終了する必要があります。この問題は、特に FI の非常に高い PV カウントまたは例外的に高い CPU 使用率の条件下で発生します。このような場合、セキュアブートアダプタがクリーンアップを完了する前にサーバ BIOS がブートシーケンスを終了すると、アダプタの検出に失敗する可能性があります。その結果、サーバが SAN から正常に起動しない場合があります。この問題は、Cisco UCS VIC 15000 シリーズアダプタを搭載したサーバの構成で発生します。	障害が発生したサーバをリブートします。	4.3(4a)

© 2025 Cisco and/or its affiliates. All rights reserved.

表 44 C シリーズ M5 サーバ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ンドル
CSCwn97854	4.3(2.240107) から 4.3(2.250016) にアップグレードするときに、Cisco UCS M5 C240 サーバでのサーバプロファイルのアクティブ化が失敗します。	**シナリオ 1：ファームウェアポリシーの使用** サーバーディスカバリが成功している場合には、次の手順を実行します。 ◦ ファームウェアポリシーを削除し、サーバープロファイルを再度アクティブにします。 ◦ サーバープロファイルの vNIC と vHBA が LCP/SCP で正しく設定されていることを確認します。 ◦ ファームウェアポリシーを使用するか、直接アップグレードワークフローを通じて、バージョン 4.3(2.250016) にアップグレードします。 **シナリオ 2：直接アップグレードを使用する** サーバを回復するには、安定した BIOS バージョンにダウングレードするか、アップグレードします。サーバーの復旧については、Cisco TAC にお問い合わせください。	4.3(2.250016)

表 45 C シリーズサーバファームウェアリリース 4.3（5.240021）で未解決の問題

不具合 ID	説明	回避策	影響を受ける最初のバンドル
CSCwk79108	同じドライブスロット上に Miami Beach Plus コントローラがあるサーバー間でのドライブの移行で、インポートされなかった仮想ドライブがリストされます。	回避策はありません。	4.3(5.240094)A

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID	説明	回避策	影響を受ける最初のバンドル
CSCwm36068	Cisco UCS M7 サーバでは、自己暗号化ドライブと非自己暗号化ドライブの組み合わせを使用したリモート対応ドライブの作成が、アウトオブバンド管理（OOB）で失敗します。この問題は、Web UI および CLI インターフェイスで発生します。	回避策はありません。	4.3(4.240152)

表 46 C シリーズ M5 サーバファームウェアリリース 4.3(2.240090) のセキュリティ修正

不具合 ID	説明	回避策	影響を受ける最初のバンドル
CSCwm55124	Broadcom/VMware データセンターの移行により、新しい Cisco UCS M5 サーバー認定は 2024 年 10 月 14 日以降にのみ開始できます。 VMware 認定および同等の証明書は、VIVa 2.0 の新しいセッションでもう一度開始される必要があります。 新しいセッションは 2024 年 10 月 14 日に開始される予定です。	回避策はありません。	4.1(3f)

表 47 C シリーズ M6 サーバファームウェア 4.3(4.242038) 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ンドル
CSCwe84825	Cisco UCS C245 M6 サーバーでは、ホストで BIOS が更新されると、構成された AMD CBS 設定ポリシーがデフォルトの状態に戻ります。	CBS 設定ポリシーを再適用して、BIOS 更新の以前の設定を保持してください。	4.3(2.230078)

表 48 C シリーズ M8 サーバファームウェアリリース 4.3(4.241014) の新しいハードウェア機能

不具合 ID	説明	回避策	影響を受ける最初のバンドル
CSCwj79250	C220 M7、C240 M7、および C245 M8 サーバで、SNMP、SMTP、および Syslog ポリシーのばらつきが断続的に確認されています。	この問題に回避策はありません。	4.3(4.240152)

© 2025 Cisco and/or its affiliates. All rights reserved.

表 49 C シリーズファームウェアリリース 4.3(3.240022) 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ンドル
CSCwi85031	Emerald Rapids 8558+、8568Y+ または CPU SKU プロセッサと 2 つの Intel Flex 170 GPU を搭載した Cisco UCS C240 M7 サーバーでクラッシュが発生し、RHEL 9.2 または Ubuntu 22.04.3 のロードに失敗しました。OS を正常に起動してインストールする代わりに、システムがハングしてクラッシュしました。	• BIOS セットアップにアクセスします。 • [詳細（Advanced）] > [ソケット構成（Socket Configuration）] > [アンコア構成（Uncore Configuration）] > [アンコア一般構成（Uncore General Configuration）] の順に選択します。 • [MMIO 高粒度サイズ（MMIO High Granularity Size）] を **1024G** に変更し、**F10** を押して保存します。 • サーバーをリブートします。	4.3(3.240022)
CSCwi85033	Emerald Rapids 8558+、8568Y+、または CPU SKU プロセッサと 2 つの NVDIA H100 GPU を搭載した Cisco UCS C240 M7 サーバーでクラッシュが発生し、RHEL 9.2 または Ubuntu 22.04.3 のロードに失敗し、運用の中断が発生しました。	◦ BIOS セットアップにアクセスします。 ◦ [詳細（Advanced）] > [ソケット構成（Socket Configuration）] > [アンコア構成（Uncore Configuration）] > [アンコア一般構成（Uncore General Configuration）] の順に選択します。 ◦ [MMIO 高粒度サイズ（MMIO High Granularity Size）] を **1024G** に変更し、**F10** を押して保存します。 ◦ サーバーをリブートします。	4.3(3.240022)

既知の問題

このセクションでは、サーバファームウェアリリースの制限について簡単に説明します。バグ ID をクリックしてバグ検索ツールにアクセスし、詳細を確認してください。

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID	症状	回避策	影響を受ける最初のバージョン
CSCwo27237	Intel(R) プロセッサを搭載した Cisco UCS X シリーズ M8 サーバに Microsoft Windows 2025(R) オペレーティングシステムをインストールし、BIOS で VMD が有効になっている場合、F6 Intel VMD ドライバのロードで通常よりも長い遅延が発生する場合があります。 NVMe ドライブの表示に必要な時間は、システムに存在する NVMe ドライブの数が原因で増加します。	Windows インストーラ画面が表示されたら、次の手順を実行します。 **[VMD ドライバをロード（Load VMD driver）]** を 1 回クリックし、3 分待ってから**[更新（Refresh）]**をクリックします。 ドライブがリストに表示されない場合は、ドライバをもう一度ロードします。エラーメッセージが表示された場合は、**[戻る（Back）]** ボタンをクリックしてディスクを再度検索します。 これで、すべての NVMe ドライブが表示されます。	5.4(0.250037)
CSCwn60053	Cisco UCS C シリーズ M8 サーバでは、改ざんされた VIC が検出されると、次のメッセージが表示されます。「信号なし。理由：ホストの電源は入っていますが、ビデオを出力していません。いずれかのキーを押してウェイクアップします。」ホスト上で POST コマンドが完了せず、全体的なシステムの正常性が [重大（Critical）] と表示されます。障害の概要には「Adapter [MLOM/ PCI] secure validation failed」というメッセージが表示されます。	回避策はありません。	4.3.5.240021
CSCwn26554	Cisco UCS C シリーズサーバでは、HSU の更新中に BMC が突然再起動した場合、次の条件でホストが再起動します。 ◦ " ApplyTime" :" OnNextBoot" and " Targets" :[" /redfish/v1/UpdateService/FirmwareInventory/BIOS" , " /redfish/v1/UpdateService/FirmwareInventory/CIMC"] ◦ " ApplyTime" :" OnNextBoot" and " Targets" :[" /redfish/v1/UpdateService/Fir	HSU 更新フローは、以下のターゲットの組み合わせに対して " ApplyTime" :" Immediate" の場合に正常に機能します。 • " Targets" : [" /redfish/v1/UpdateService/FirmwareInventory/BIOS" ," /redfish/v1/UpdateService/FirmwareInventory/CIMC"]] • " Targets" :[" /redfish/v1/UpdateService/FirmwareInventory/BIOS"]] '。 • " Targets" :[" /redfish/v1/UpdateService/FirmwareInventory/CIMC"]}'。	4.3.5.240021

© 2025 Cisco and/or its affiliates. All rights reserved.

不具合 ID	症状	回避策	影響を受ける最初のバージョン
	mwareInventory/BIOS"] ◦ " ApplyTime" :" OnNextBoot" and " Targets" : [" /redfish/v1/UpdateService/FirmwareInventory/CIMC"]		
CSCwn36143	Genoa 1U NVMe SKU を搭載した Cisco UCS C225 M8 サーバでは、NVMe ドライブのホットプラグ中に PCIe PERR エラーが観察されます。	回避策はありません。 これらのエラーは SEL 警告であり、機能に影響がないため無視してかまいません。	4.3.5.240021

互換性

このセクションでは、サーバファームウェアリリースの互換性情報を示します。

クロスバージョンファームウェアサポート

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)
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）	なし	○	○	○	○	○	○	○	○
5.0(2)	なし	○	○	○	非対応	非対応	非対応	非対応	非対応

© 2025 Cisco and/or its affiliates. All rights reserved.

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)
5.0(1)	なし	○	○	○	非対応	非対応	非対応	非対応	非対応

C 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)
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
4.2(1)	○	○	○	○	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

B 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)
5.4(0)	○	○	○	○	○	○	○	○	○
5.3(0)	○	○	○	○	○	○	○	○	○
5.2(2)	○	○	○	○	○	○	○	○	○

© 2025 Cisco and/or its affiliates. All rights reserved.

B 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)
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

関連技術情報

- Cisco Intersight のリリースノートとリリースバンドル
- Cisco Intersight、Cisco IMC、および Cisco UCS Manager 向け Cisco UCS 同等性マトリクス
- Cisco Intersight のリリースノートとリリースバンドル
- 『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 C885A M8 ラックサーバの Cisco Baseboard Management Controller リリースノート
- Cisco UCS Manager と Intersight のリリース戦略
- Intersight 管理モードでのファームウェアの管理

法的情報

シスコおよびシスコのロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商標または商標です。シスコの商標の一覧については、https://www.cisco.com/c/ja_jp/about/legal/trademarks.html をご覧ください。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2025 Cisco Systems, Inc. All rights reserved.

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。