Cisco Integrated Management Controller の特権昇格の脆弱性

アドバイザリーID : cisco-sa-ucs-ssh-priv-esc-2mZDtdjM
初公開日 : 2025-06-04 16:00
バージョン 1.0 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID : CSCwk24502 CSCwc06871

CVE-2025-20261

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

Cisco UCS Bシリーズ、UCS Cシリーズ、UCS Sシリーズ、およびUCS Xシリーズサーバ用のCisco Integrated Management Controller(IMC)のSSH接続処理における脆弱性により、認証されたリモートの攻撃者が、昇格された特権を使用して内部サービスにアクセスする可能性があります。

この脆弱性は、内部サービスへのアクセスの制限が不十分であることに起因します。有効なユーザアカウントを持つ攻撃者が、SSHを介して該当デバイスのCisco IMCに接続する際に、巧妙に細工された構文を使用することで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は昇格された権限を使用して内部サービスにアクセスし、該当デバイスで新しい管理者アカウントを作成するなど、システムに不正な変更を加える可能性があります。

シスコはこの脆弱性に対処するソフトウェアアップデートをリリースしています。この脆弱性に対処する回避策はありませんが、回避策はあります。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-ssh-priv-esc-2mZDtdjM

該当製品

脆弱性のある製品

この脆弱性は、脆弱性のあるソフトウェアリリースを実行し、Cisco IMCへの着信SSH接続を受け入れる次のシスコ製品に影響を与えます。

- UCS Bシリーズブレードサーバ(CSCwk24502)
- UCS Cシリーズラックサーバ(CSCwc06871)
- UCS Sシリーズストレージサーバ(CSCwc06871)
- UCS Xシリーズモジュラシステム(CSCwk24502)

注：スタンドアロンモードのCisco UCS CシリーズおよびUCS Sシリーズサーバは、デフォルトで着信SSH接続を受け入れます。詳細については、『Cisco UCS CシリーズIntegrated Management Controller GUIコンフィギュレーションガイド』の「SSHの設定」セクションを参照してください。Cisco UCS Bシリーズ、マネージドUCS Cシリーズ、マネージドUCS Sシリーズ、およびUCS Xシリーズサーバは、関連付けられたサービスプロファイルでSerial over LAN(SoL)ポリシーが有効になっている場合にのみ、着信SSH接続を受け入れます。詳細については、『Cisco UCS Managerサーバ管理ガイド』の「Serial over LANポリシーの設定」セクションを参照してください。

Cisco UCS Cシリーズサーバの事前設定バージョンに基づくCiscoアプライアンスでも、Cisco IMCへのSSHアクセスが可能な場合、この脆弱性の影響を受けます。公表時点では、次のシスコ製品が含まれていました。

- Application Policy Infrastructure Controller(APIC)サーバ
- Business Edition 6000および7000アプライアンス
- Catalyst Center Appliances（旧DNA Center）
- Cisco Telemetry Brokerアプライアンス
- Cloud Services Platform(CSP)5000シリーズ
- Common Services Platform Collector(CSPC)アプライアンス
- コネクテッドモバイルエクスペリエンス(CMX)アプライアンス
- Connected Safety and Security UCSプラットフォームシリーズサーバ
- Cyber Vision Centerアプライアンス
- Expresswayシリーズアプライアンス
- HyperFlex Edgeノード
- HyperFlexノード
- IEC6400エッジコンピューティングアプライアンス
- IOS XRv 9000アプライアンス
- Meeting Server 1000アプライアンス
- Nexusダッシュボードアプライアンス
- Prime Infrastructureアプライアンス
- Prime Network Registrar Jumpstartアプライアンス
- セキュアエンドポイントプライベートクラウドアプライアンス
- Secure Firewall Management Centerアプライアンス（旧称：Firepower Management Center）
- セキュアマルウェア分析アプライアンス
- Secure Network Analyticsアプライアンス
- Secure Network Serverアプライアンス

- 安全なワークロードサーバ

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- 5000シリーズエンタープライズネットワークコンピューティングシステム(ENCS)
- Catalyst 8300シリーズEdge uCPE
- UCS E シリーズ サーバ

回避策

この脆弱性に対処する回避策はありません。ただし、緩和策があります。

これが必要でない場合、該当するデバイスのCisco IMCへのSSHアクセスが無効になる場合があります。

スタンドアロンモードのCisco UCS CシリーズおよびUCS Sシリーズサーバの場合、Cisco IMC Web UIでAdmin > Communication Servicesの順に選択し、SSH Enabledオプションのチェックマークを外します。

Cisco UCS Bシリーズ、マネージドUCS Cシリーズ、マネージドUCS Sシリーズ、およびUCS Xシリーズサーバでは、関連付けられたサービスプロファイルでSerial over LAN(SoL)ポリシーを無効にします（SoLアクセスはデフォルトで無効になっています）。 Cisco UCS Manager Web UIのServersセクションで、次の操作を実行します。

1. 問題のサービスプロファイルを選択します。
2. PoliciesタブのActionsにあるChange Serial over LAN Policyリンクをクリックします。
3. No Serial over LAN Policyオプションを選択します。
4. [OK] をクリックします。

または、Policies > Serial over LAN Policiesの順に選択して、適用されたSerial over LAN Policyを編集し、Serial over LAN StateプロパティをEnableからDisableに変更します。これにより、対象のSoLポリシーを使用しているすべてのサービスプロファイルでSoLアクセスが無効になります。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環

境への適用性と環境への影響を評価した後で導入してください。

修正済みソフトウェア

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次の表では、左の列にシスコソフトウェアのリリースを記載しています。右側の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。

UCS ManagerモードのUCS BシリーズおよびXシリーズサーバ

Cisco UCSサーバソフトウェアリリース	First Fixed Release（修正された最初のリリース）
4.1 より前	修正済みリリースに移行。
4.1	4.1(3n)
4.2	4.2(3k)
4.3	4.3(4c)

IntersightマネージドモードのUCS Bシリーズサーバ

Cisco Intersightサーバファームウェアリリース	First Fixed Release（修正された最初のリリース）
4.2 より前	修正済みリリースに移行。
4.2	4.2(3i)
5.1	修正済みリリースに移行。
5.2	5.2（2.240073）
5.3	脆弱性なし
5.4	脆弱性なし

IntersightマネージドモードのUCS Xシリーズサーバ

Cisco Intersightサーバファームウェアリリース	First Fixed Release（修正された最初のリリース）
5.0	5.0(4f)
5.1	修正済みリリースに移行。
5.2	5.2（2.240073）
5.3	脆弱性なし
5.4	脆弱性なし

スタンドアロンモードまたはIntersightマネージドモードのUCS CシリーズおよびSシリーズサーバ

Cisco UCSサーバソフトウェアリリース	First Fixed Release（修正された最初のリリース）
4.2 より前	修正済みリリースに移行。
4.2	4.2(2f)、4.2(3b)
4.3	脆弱性なし

UCS ManagerモードのUCS CシリーズおよびSシリーズサーバ

Cisco UCSサーバソフトウェアリリース	First Fixed Release（修正された最初のリリース）
4.2 より前	修正済みリリースに移行。
4.2	4.2(2c)、4.2(3b)
4.3	脆弱性なし

注：事前設定バージョンのCisco UCS Cシリーズサーバに基づくCiscoアプライアンスでは、管理者はCisco IMCソフトウェアを、上の表に示した修正済みリリースのいずれかに直接アップグレードできます。手順については、『Cisco Host Upgrade Utility User Guide』を参照してください。ただし、次の表に記載されているアプライアンスは例外です。これらのアプライアンスについては、「修復」列の指示に従ってください。

シスコ ハードウェア プラットフォーム	修復方法
Cisco Telemetry Brokerアプライアンス	ファームウェアアップデートm6-tb2300-ctb-firmware-4.3-2.240009.iso以降を適用します。
IEC6400エッジコンピューティングアプライアンス	IEC6400-HUU-4.2.3j.imgを使用してHUUアップグレードを適用します。
セキュアエンドポイントプライベートクラウドアプライアンス	TechNoteに記載されている手順に従ってください。
Secure Firewall Management Centerアプライアンス	ホットフィックスEN以降を適用します。
セキュアマルウェア分析アプライアンス	リリース2.19.4以降にアップグレードするには、「ファームウェアの更新」の手順に従ってください。
Secure Network Analyticsアプライアンス	アップデートパッチpatch-common-SNA-FIRMWARE-20240305-v2-01.swu以降をインストールします。
Secure Network Serverアプライアンス	『Cisco SNS 3700シリーズのファームウェアアップグレードガイド』または『Cisco SNS 3600シリーズ』の説明に従って、BIOSおよびHUUアップグレードを適用します。

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

出典

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-ssh-priv-esc-2mZDtdjM

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2025年6月4日

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。