Cisco Integrated Management Controller CLI のコマンド インジェクションにおける脆弱性

アドバイザリーID : cisco-sa-cimc-cmd-inj-mUx4c5AJ
CVE-2024-20295
初公開日 : 2024-04-17 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 : CSCwi10842 CSCwi12864 CSCwi29799

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 Integrated Management Controller(IMC)のCLIにおける脆弱性により、認証されたローカルの攻撃者が、基盤となるオペレーティングシステムに対してコマンドインジェクション攻撃を実行し、権限をrootに昇格させる可能性があります。この脆弱性を不正利用するには、攻撃者は該当デバイスで読み取り専用以上の権限を持っている必要があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、細工された CLI コマンドを送信することで、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 root に特権昇格できるようになります。

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。

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-cimc-cmd-inj-mUx4c5AJ

該当製品

脆弱性のある製品

この脆弱性は、デフォルト設定でCisco IMCの脆弱性のあるリリースを実行している次のシスコ製品に影響を与えます。

- 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
- スタンドアロンモードになっている UCS C シリーズ ラックサーバ
- UCS E シリーズ サーバ

事前設定されたバージョンのCisco UCS Cシリーズサーバをベースとするシスコアプライアンスも、Cisco IMC CLIへのアクセスが可能な場合は影響を受けます。このドキュメントの発行時点で、これには次のシスコ製品が含まれていました。

- 5520および8540ワイヤレスコントローラ
- Application Policy Infrastructure Controller(APIC)サーバ
- Business Edition 6000および7000アプライアンス
- Catalyst Centerアプライアンス(旧称DNA Center(DNAC))
- 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センターアプライアンス
- Expresswayシリーズアプライアンス
- HyperFlex Edgeノード
- ファブリックインターコネクト(DC-NO-FI)導入モードを使用しないHyperFlexデータセンターの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Eメールゲートウェイ[1]
- セキュアEメールおよびWebマネージャ[1]
- 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
- セキュアWebアプライアンス[1]
- 安全なワークロードサーバ
- テレメトリブローカアプライアンス

1. Cisco IMCはこれらのアプライアンスから直接アクセスできないため、これらのプラットフォームでの攻撃ベクトルが大幅に減少します。

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。

注：シスコポートフォリオの簡素化の一環として、セキュリティ製品の名称を変更し、Cisco Secure というブランド名に統一しています。詳細については、「Cisco Secure が登場」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記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

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。

- UCS B シリーズ ブレード サーバ
- Cisco UCS Managerで管理されるUCS Cシリーズラックサーバ
- UCS S シリーズ ストレージ サーバ
- UCS Xシリーズモジュラシステム

回避策

この脆弱性に対処する回避策はありません。

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アップグレード ソリューション一式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。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco 5000シリーズENCSおよびCatalyst 8300シリーズEdge uCPE

注：Cisco 5000シリーズENCSおよびCisco Catalyst 8300シリーズエッジuCPEでCisco IMCをアップグレードするには、プラットフォームでCisco Enterprise NFVインフラストラクチャソフトウェア(NFVIS)をアップグレードする必要があります。Cisco IMCは、ファームウェア自動アップグレードプロセスの一部としてアップグレードされます。

Cisco NFVISリリース	First Fixed Release（修正された最初のリリース）
3.12 以前	修正済みリリースに移行。
4.13 以前	4.14.1

Cisco UCS CシリーズM4ラックサーバ

Cisco IMCリリース	First Fixed Release（修正された最初のリリース）
4.0 以前	修正済みリリースに移行。

Cisco IMCリリース	First Fixed Release（修正された最初のリリース）
4.1	4.1(2m)

Cisco UCS CシリーズM5ラックサーバ

Cisco IMCリリース	First Fixed Release（修正された最初のリリース）
4.0 以前	修正済みリリースに移行。
4.1	4.1(3m)
4.2	4.2(3j)
4.3	4.3（2.240002）

Cisco UCS CシリーズM6ラックサーバ

Cisco IMCリリース	First Fixed Release（修正された最初のリリース）
4.2	4.2(3j)
4.3	4.3（2.240002）

Cisco UCS CシリーズM7ラックサーバ

Cisco IMCリリース	First Fixed Release（修正された最初のリリース）
4.3	4.3（2.240002）

Cisco UCS EシリーズM2およびM3

Cisco IMCリリース	First Fixed Release（修正された最初のリリース）
3.2.4 以前	脆弱性なし
3.2.6 以降	3.2.15

Cisco UCS EシリーズM6

Cisco IMCリリース	First Fixed Release（修正された最初のリリース）
4.12 以前	4.12.2

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シスコアプライアンスについては、管理者はCisco IMCソフトウェアを、上記の表に記載され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ユーザガイド』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	最初の修正済みCisco IMCリリース	修復方法
IEC6400エッジコンピューティングアプライアンス	4.2(3j)	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Eメールゲートウェイ	4.2(3j)	ファームウェアアップデートパッケージのインストール（2024年5月）
Cisco Secure Email and Web Manager	4.2(3j)	ファームウェアアップデートパッケージのインストール（2024年5月）
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	4.3（2.240009）	ファームウェアアップデートucs-firmware-4.3.2.240009-1.rpmをインストールします（2024年5月）。
Secure Firewall Management Centerアプライアンス	4.3（2.240009）	ホットフィックスEZを適用します。
セキュアマルウェア分析アプライアンス	4.3（2.240009）	リリース2.19.3（2024年7月）にアップグレードします。
Secure Network Analyticsアプライアンス	4.1(2m)(M4) 4.3(2.240009)(M5、M6)	アップデートucs-c220m4-huu-4.1.2m-sna.iso(M4)またはucs-c240m4-huu-4.1.2m-sna.iso(M4)を適用します。 アップデートパッチpatch-common-SNA-FIRMWARE-20240305-v2-01.swu(M5、M6)をインストールします。
Secure Network Serverアプライアンス	4.3（2.240009）	『Firmware Upgrade Guide for SNS 3700 Series or SNS 3600 Series』に記載されているように、BIOSおよびHUUのアップグレードを適用します。
セキュアWebアプライアンス	4.2(3j)	ファームウェアアップデートパッケージのインストール（2024年5月）

シスコ ハードウェア プラットフォーム	最初の修正済みCisco IMCリリース	修復方法
テレメトリブローカアプライアンス	4.3（2.240009）	アップデートpatch-common-CTB-FIRMWARE-20240305.isoを適用します。

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された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 は、このアドバイザリで説明されている脆弱性に対してコンセプト実証エクスプロイトコードが利用可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

この脆弱性を報告していただいたセキュリティ研究者のJames Muller氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-mUx4c5AJ

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	2024年4月17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。