

Cisco Integrated Management Controller の Web ベース管理インターフェイスにおけるコマンドインジェクションへの脆弱性



アドバイザリーID : cisco-sa-cimc-cmd-inj- [CVE-2024-
bLuPcb](#) [20356](#)

初公開日 : 2024-04-17 16:00

最終更新日 : 2024-04-19 16:36

バージョン 1.1 : Final

CVSSスコア : [8.7](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwi43001](#) [CSCwj41082](#)

[CSCwi42996](#) [CSCwi43005](#)

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Webベースの管理インターフェイスにおける脆弱性により、管理者レベルの権限を持つ認証されたリモートの攻撃者が、該当システムで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。

この脆弱性は、不十分なユーザの入力検証に起因します。攻撃者は、巧妙に細工されたコマンドを該当するソフトウェアの Web ベース管理インターフェイスに送信することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は権限を root に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。

このアドバイザリーは、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-bLuPcb>

該当製品

脆弱性のある製品

この脆弱性による影響を受けるのは、次のシスコ製品で、Cisco IMC の脆弱性のあるリリース

をデフォルト設定で実行している場合です。

- 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 エッジ uCPE
- スタンドアロンモードの Cisco UCS C シリーズ M5、M6、および M7 ラックサーバー
- UCS E シリーズ サーバ
- スタンドアロンモードの UCS S シリーズ ストレージ サーバー

上記のリストに含まれる Cisco UCS C シリーズ サーバーの事前設定済みバージョンをベースとするシスコアプライアンスも、Cisco IMC UI へのアクセスを公開している場合は、この脆弱性の影響を受けます。本ドキュメントの発行時点で、これに該当するシスコ製品は次のとおりです。

- Application Policy Infrastructure Controller (APIC) サーバー
- Business Edition 6000 および 7000 アプライアンス
- Cisco Catalyst Center アプライアンス (旧称 : Cisco 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
- Connected Mobile Experiences (CMX) アプライアンス
- Cisco Connected Safety and Security UCS プラットフォーム シリーズ サーバー
- Cyber Vision Center アプライアンス
- Expressway シリーズ アプライアンス
- HyperFlex エッジノード
- ファブリック インターコネクトを使用しない HyperFlex データセンター (DC-NO-FI) 展開モードの HyperFlex ノード
- IEC6400 エッジ コンピューティング アプライアンス
- Cisco IOS XRv 9000 アプライアンス
- Meeting Server 1000 アプライアンス
- Nexus Dashboard 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
- Cisco Secure Email Gateway¹
- Cisco Secure Email and Web Manager¹
- Cisco Secure Endpoint Private Cloud アプライアンス
- Cisco Secure Firewall Management Center アプライアンス (旧称 : Firepower Management Center)
- Cisco Secure Malware Analytics アプライアンス
- Secure Network Analytics アプライアンス
- Cisco Secure Network Server アプライアンス
- Cisco Secure Web アプライアンス¹
- Cisco Secure Workload サーバー

1. これらのアプライアンスから Cisco IMC に直接アクセスすることはできないため、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、本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 の管理対象である UCS C シリーズ ラックサーバー
- Cisco UCS Manager の管理対象である UCS S シリーズ ストレージ サーバー
- UCS X シリーズ モジュラーシステム

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ン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です。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 Cisco Catalyst 8300 シリーズエッジ 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、プラットフォームの 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、ファームウェアの自動アップグレードプロセスの一環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 M5 ラックサーバー

Cisco IMC のリリース	First Fixed Release (修正された最初のリリース)
4.0	修正済みリリースに移行。
4.1	4.1(3n)
4.2	4.2(3j)
4.3	4.3 (2.240009)

Cisco UCS C シリーズ M6 ラックサーバー

Cisco IMC のリリース	First Fixed Release (修正された最初のリリース)
4.2	4.2(3j)
4.3	4.3 (2.240009) 4.3 (3.240022)

Cisco UCS C シリーズ M7 ラックサーバー

Cisco IMC のリリース	First Fixed Release (修正された最初のリリース)
4.3	4.3 (3.240022)

UCS E シリーズ M2 および M3 サーバー

Cisco IMC のリリース	First Fixed Release (修正された最初のリリース)
3.1 以前	修正済みリリースに移行。
3.2	3.2.15.3

UCS E シリーズ M6 サーバー

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

UCS S シリーズ ストレージ サーバー

Cisco IMC のリリース	First Fixed Release (修正された最初のリリース)
4.0	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 (2.240009) 4.3 (3.240041)

注：上記の表に示した Cisco UCS C シリーズ サーバーの事前設定済みバージョンをベースにし

たシスコアプライアンスについては、Cisco IMC ソフトウェアを上記の表に記載の修正済みリリースのいずれかに管理者が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、「修復方法」の欄にある手順に従ってください。

シスコ ハードウェア プラットフォーム	最初に修正された Cisco IMC リリース	修復方法
Cisco Telemetry Broker アプライアンス	4.3 (2.240009)	更新 m6-tb2300-ctb-firmware-4.3-2.240009.iso 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	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。
Cisco Secure Email Gateway	4.2(3j)	ファームウェア更新パッケージ (2024 年 5 月) をインストールします。
Cisco Secure Email and Web Manager	4.2(3j)	ファームウェア更新パッケージ (2024 年 5 月) をインストールします。
Cisco Secure Endpoint Private Cloud アプライアンス	4.3 (2.240009)	ファームウェア更新 ucs-firmware-4.3.2.240009-1.rpm (2024 年 5 月) をインストールします。
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。
Cisco Secure Malware Analytics 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	4.3 (2.240009)	更新パッチ patch-common-SNA-FIRMWARE-20240305-v2-01.swu をインストールします。
Cisco 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 』の説明に従って、BIOS および HUU のアップグレードを適用します。

シスコ ハードウェア プラットフォーム	最初に修正された Cisco IMC リリース	修復方法
Cisco Secure Web Appliance	4.2(3j)	ファームウェア更新パッケージ (2024 年 5 月) をインストールします。

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

シスコは、この脆弱性を報告していただいた LRQA Nettitude 社の Aaron Thacker 氏に感謝いたします。

URL

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

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	Cisco Telemetry Broker アプライアンスのパッチ名を更新。パッチのダウンロード手順へのリンクを追加。コンセプト実証コードの通知を追加。	対象リリース、修正済みリリース、不正利用事例と公式発表	Final	2024 年 4 月 19 日
1.0	初回公開リリース	—	Final	2024 年 4 月 17 日

利用規約

本アドバイザーは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザーの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

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。