# 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
最終更新日 : 2024-06-28 15:22
バージョン 1.2 : 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 コマンド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。この脆弱性をエクスプロイトするには、攻撃者は該当デバイスの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

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 CLI へのアクセスを公開している場合は影響を受けます。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。

- 5520 および 8540 ワイヤレスコントローラ
- 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（DNAC））
- 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 Gateway[1]
- Cisco Secure Email and Web Manager[1]
- 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、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 の管理対象である UCS C シリーズ ラックサーバー
- UCS S シリーズ ストレージ サーバ
- 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 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 M4 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 以前 | 修正済みリリースに移行。 |

| Cisco IMC のリリース | 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 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 ( 2.240002 ) |

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 ( 2.240002 ) |

Cisco UCS E シリーズ M2 および M3

| Cisco IMC のリリース | 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 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 |

注： 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を使用したHUUアップグレードの適用 |
| Cisco Secure Email Gateway | 4.2(3j) | Cisco IMCファームウェアアップデートパッケージをインストールします。 |
| Cisco Secure Email and Web Manager | 4.2(3j) | Cisco IMCファームウェアアップデートパッケージ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 ) | 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 | 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2.19.4 ( 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)<br><br>4.3(2.240009) (M5, M6) | 更新 ucs-c220m4-huu-4.1.2m-sna.iso または ucs-c240m4-huu-4.1.2m-sna.iso ( M4 ) を適用します。<br><br>更新パッチ patch-common-SNA-FIRMWARE-20240305-v2-01.swu ( M5、M6 ) をインストールします。 |
| Cisco Secure Network Server アプライアンス | 4.1(2m) (M4)<br><br>4.3(2.240009)(M5、M6) | Cisco SNS 3500シリーズ用の4.1(2m)ファームウェアリリースをインストールしてアクティブ化します。<br><br>『Cisco SNS 3700シリーズ』または『Cisco SNS 3600シリーズのファームウ |

| 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 |
| --- | --- | --- |
| | | エアアップグレードガイド』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。 |
| Cisco Secure Web Appliance | 4.2(3j) | Cisco IMCファームウェアアップデートパッケージ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

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 |
| --- | --- | --- | --- | --- |
| 1.2 | 修正済みリリースと修正情報を更新。 | 修正済みリリース | Final | 2024年6月28日 |
| 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。 | 該当製品および修正済みリリース | Final | 2024 年 4 月 19 日 |
| 1.0 | 初回公開リリース | — | Final | 2024 年 4 |

| バージョン | 説明 | セクション | ステータス | 日付 |
| --- | --- | --- | --- | --- |
| | | | | 月 17 日 |

## 利用規約

本アドバイザリ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。 本アドバイザリ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。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、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。