Cisco Integrated Management Controllerのコマンドインジェクションとリモートコード実行の脆弱性

High

アドバイザリーID : cisco-sa-cimc-cmd-inj-3hKN3bVt
初公開日 : 2026-04-01 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 : CSCwr60925 CSCws00378 CSCwr60021 CSCws00368 CSCws00363 CSCwr60889 CSCws00376 CSCws00370 CSCwr60894

CVE-2026-20095
CVE-2026-20096
CVE-2026-20094
CVE-2026-20097

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複数の脆弱性により、認証されたリモートの攻撃者が、該当システムの基盤となるオペレーティングシステムで任意のコードまたはコマンドを実行し、権限をrootに昇格させる可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これら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-3hKN3bVt

該当製品

脆弱性のある製品

これらの脆弱性は、デバイス設定に関係なく、Cisco IMCの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えます。

製品	CVE ID	Cisco Bug ID
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）	CVE-2026-20095 CVE-2026-20096	CSCws00370 CSCws00378
Catalyst 8300 シリーズ エッジ uCPE	CVE-2026-20094 CVE-2026-20095 CVE-2026-20096	CSCws00363 CSCws00368 CSCws00376
スタンドアロンモードのUCS CシリーズM5およびM6ラックサーバ	CVE-2026-20094 CVE-2026-20095 CVE-2026-20096 CVE-2026-20097	CSCwr60021 CSCwr60889 CSCwr60894 CSCwr60925
UCS E シリーズ サーバー M3	CVE-2026-20095 CVE-2026-20096	CSCws00370 CSCws00378
UCS EシリーズサーバM6	CVE-2026-20094 CVE-2026-20095 CVE-2026-20096	CSCws00363 CSCws00368 CSCws00376
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	CVE-2026-20094 CVE-2026-20095 CVE-2026-20096	CSCwr60021 CSCwr60889 CSCwr60894

上記のリストに含まれるCisco UCS Cシリーズサーバの事前に設定されたバージョンに基づくCiscoアプライアンスも、Cisco IMC UIへのアクセスが可能な場合、これらの脆弱性の影響を受けます。これには、次のシスコ製品が含まれます。

- 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(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
- 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 Endpoint Private Cloud アプライアンス
- Cisco Secure Firewall Management Center アプライアンス
- Cisco Secure Malware Analytics アプライアンス
- Cisco Secure Network Analytics アプライアンス
- Cisco Secure Network Server アプライアンス
- Cisco Secure Workload サーバー

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」セクションに記載されている製品のみが、これら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、次のシスコ製品がこれらの脆弱性の影響を受けないことを確認しました。

- UCS B シリーズ ブレード サーバ
- UCS CシリーズM7およびM8ラックサーバ
- UCS Cシリーズラックサーバ(UCS ManagerまたはIntersight Managed Mode(IMM)内のファブリックインターコネクト搭載)
- UCS Xシリーズモジュラシステム
- 統合されたエッジ

シスコは、CVE-2026-20094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ENCS
- UCS E シリーズ サーバー M3
- UCS ManagerまたはIntersightマネージドモード(IMM)でファブリックインターコネクトを使用したUCS Sシリーズストレージサーバ

シスコは、CVE-2026-20095およびCVE-2026-20096がUCS ManagerまたはIntersight Managed Mode(IMM)でファブリックインターコネクトを備えたUCS Sシリーズストレージサーバには影響しないと判断しました。

シスコは、CVE-2026-20097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ENCS
- Catalyst 8300 シリーズ エッジ uCPE
- UCS E シリーズ サーバ
- UCS S シリーズ ストレージ サーバ

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2026-20094:Cisco IMCのコマンドインジェクションの脆弱性

Cisco IMCのWebベース管理インターフェイスにおける脆弱性により、読み取り専用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、rootユーザとして任意のコマンドを実行する可能性があります。

この脆弱性は、ユーザー入力の検証が不適切なことに起因します。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、攻撃者はルートユーザとして基盤となるオペレーティングシステムで任意のコマンドを実行でき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。

バグID: CSCwr60021、CSCws00363
CVE ID：CVE-2026-20094
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2026-20095およびCVE-2026-20096:Cisco IMCのコマンドインジェクションの脆弱性

Cisco IMCのWebベース管理インターフェイスにおける2つの脆弱性により、adminレベルの権限を持つ認証されたリモートの攻撃者が、該当システムに対してコマンドインジェクション攻撃を実行し、rootユーザとして任意のコマンドを実行できる可能性があります。

これらの脆弱性は、ユーザ入力の検証が不適切なことに起因します。攻撃者は、巧妙に細工されたコマンドを該当ソフトウェアのWebベースの管理インターフェイスに送信することで、これら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、攻撃者はルートユーザとして基盤となるオペレーティングシステムで任意のコマンドを実行できる可能性があります。

シスコでは、これらの脆弱性に対し、スコアに示されているように「中」ではなく「高」のセキュリティ影響評価(SIR)を割り当てています。これは、攻撃者がルートになると、セキュリティに対する追加の影響が発生する可能性があるためです。

シスコはこれら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。これらの脆弱性に対処する回避策はありません。

バグID: CSCwr60889、CSCws00368、CSCws00370、CSCwr60894、CSCws00376、CSCws00378
CVE ID：CVE-2026-20095、CVE-2026-20096
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：6.5
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

CVE-2026-20097:Cisco IMCのリモートコード実行の脆弱性

Cisco IMCのWebベース管理インターフェイスの脆弱性により、adminレベルの権限を持つ認証されたリモートの攻撃者が、rootユーザとして任意のコードを実行できる可能性があります。

この脆弱性は、Webベースの管理インターフェイスに対するユーザ入力の検証が不適切なことに起因します。攻撃者は、該当デバイスに巧妙に細工された HTTP 要求を送信することにより、この脆弱性をエクスプロイトすることができます。エクスプロイトに成功すると、攻撃者はルートユーザとして基盤となるオペレーティングシステムで任意のコードを実行できる可能性があります。

シスコはこの脆弱性を「中」ではなく「高」のSIRとしてスコアに割り当てました。これは、攻撃者がルートになると、追加のセキュリティ影響が発生する可能性があるためです。

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。

バグID: CSCwr60925
CVE ID：CVE-2026-20097
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：6.5
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N

回避策

これら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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。これらの脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨し

ます。

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、およびこれら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。

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、ファームウェアの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	第1修正済みリリース(ENCS)
4.15 以前	4.15.5

Cisco NFVIS リリース	最初の修正済みリリース(uCPE)
4.16 以前	修正済みリリースに移行。
4.18	4.18.3 (Apr 2026)
26.1	脆弱性なし

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）
4.2 以前	修正済みリリースに移行。
4.3	4.3（2.260007）

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 以前	修正済みリリースに移行。
4.3	4.3（6.260017）
6.0	6.0（2.260044）

UCS EシリーズM3

Cisco IMCリリース	First Fixed Release（修正された最初のリリース）
3.2 以前	3.2.17

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）
4.15 以前	4.15.3

UCS Sシリーズストレージサーバ

Cisco IMCリリース	First Fixed Release（修正された最初のリリース）
4.2 以前	修正済みリリースに移行。
4.3	4.3（6.260017）

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(HUU)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	6.0(2.260044)(M6)	ファームウェアアップデートm6-tb2300-ctb-firmware-6.0-2.260044.isoを適用します（2026年4月）。
IEC6400 エッジ コンピューティング アプライアンス	4.3(6.260017)(M6)	IEC6400-HUU-4.3.6.imgを使用してHUUアップグレードを適用します。
Cisco Secure Endpoint Private Cloud アプライアンス	4.3(2.260007)(M5) 4.3(6.260017)(M6)	リリース4.2.5以降にアップグレードし、『TechNote』に記載されている手順に従ってください。
Cisco Secure Firewall Management Center アプライアンス	4.3(2.260007)(M5) 4.3(6.260017)(M6)	ホットフィックスFXを適用します。
Cisco Secure Malware Analytics アプライアンス	4.3(2.260007)(M5) 4.3(6.260017)(M6)	アウトオブバンド ファームウェアの更新 ISO の手順を使用して、ファームウェアを更新します。

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 Network Analytics アプライアンス	4.3(2.260007)(M5) 6.0(2.260044)(M6)	M5に対して、patch-common-SNA-FIRMWARE-20260210-M5-REL.isoをインストールします。 M6については、2026年4月にパッチがリリースされる予定です。
Cisco Secure Network Server アプライアンス	4.3(2.260007)(M5) 4.3(6.260017)(M6) 6.0(2.260044)(M6)	『Cisco Secure Network Server 3600シリーズまたはCisco Secure Network Server 3700シリーズのファームウェアアップグレードガイド』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。

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とその公表は確認しておりません。

出典

これらの脆弱性を報告していただいたポーランドのINGハブのGrzegorz Misiun氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-3hKN3bVt

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	2026年4月1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。