Cisco Integrated Management Controllerのクロスサイトスクリプティングの脆弱性

Medium

アドバイザリーID : cisco-sa-cimc-xss-7EhBFxBp
初公開日 : 2026-08-05 16:00
バージョン 1.0 : Final
CVSSスコア : 4.8
回避策 : No workarounds available
Cisco バグ ID : CSCwt96899 CSCwu66661 CSCwu66669

CVE-2026-20198

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ベース管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、インターフェイスのユーザに対してクロスサイトスクリプティング(XSS)攻撃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十分なことに起因します。攻撃者は、細工されたリンクをクリックするように該当インターフェイスのユーザを誘導することで、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、攻撃者はターゲットユーザのブラウザで任意のスクリプトコードを実行したり、ブラウザの機密情報にアクセスしたりす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。

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-xss-7EhBFxBp

該当製品

脆弱性のある製品

公開時点では、デバイスの設定にかかわらず、次のシスコ製品でCisco IMCの脆弱性のあるリリースが実行されている場合、この脆弱性の影響を受けました。

- 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)(CSCwu66661)
- Catalyst 8300シリーズEdge uCPE(CSCwu66669)
- 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(CSCwt96899)
- UCS Eシリーズサーバ M3(CSCwu66661)
- UCS Eシリーズサーバ M6(CSCwu66669)
- 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(CSCwt96899)

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、これら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
- Catalyst Center アプライアンス
- 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 Endpoint Private Cloud アプライアンス
- Secure Firewall Management Center(FMC)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
- Secure Network Server(ISE SNS)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、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
- スタンドアロンモードの Cisco UCS C シリーズ M7 および M8 ラックサーバー
- ファブリック インターコネクトに接続した、UCS Manager または Intersight 管理モード（IMM）の UCS C シリーズ ラックサーバー
- ファブリック インターコネクトに接続した、UCS Manager または Intersight 管理モード（IMM）の 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
- Unified Edge

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

公開時点では、次の表のリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

左側の列にはシスコソフトウェアリリース、右側の列に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リリースが示されています。

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	最初の修正済みリリース（ENCS）
4.12 より前	修正済みリリースに移行。
4.12	4.12.8
4.13	修正済みリリースに移行。
4.14	修正済みリリースに移行。
4.15	4.15.6

Cisco NFVIS リリース	最初の修正済みリリース（uCPE）
4.12	4.12.8
4.13	修正済みリリースに移行。
4.14	修正済みリリースに移行。
4.15	4.15.6
4.16	修正済みリリースに移行。
4.18	4.18.5（2026年9月）
26.1	26.1.2

Cisco UCS C シリーズ M5 ラックサーバー

Cisco UCS サーバー 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(3r)
4.3	4.3（2.260020）

Cisco UCS C シリーズ M6 ラックサーバー

Cisco UCS サーバー 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(3r)
4.3	4.3（6.260054）
6.0	6.0(2.260143)[1]

1. 修正済みの 6.0(2.260143) Host Upgrade Utility(HUU)ISOリリースには、Cisco IMC 6.0(2.260094)パッケージリリースが含まれています。この修正済みリリースにアップグレードすると、Cisco IMC UI Dashboardページの Firmware Versionに6.0(2.260094)が表示されます。Administration > Firmware Managementの下の Last HSU bundle usedフィールドに、修正済みの6.0(2.260143)リリースが表示されます。

UCS E シリーズ M3

Cisco UCSE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）
3.2 以前	3.2.18.1

UCS E シリーズ M6

Cisco UCSE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）
4.15 以前	4.15.4

UCS S シリーズ ストレージ サーバー

Cisco UCS サーバー 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）
4.3 より前	修正済みリリースに移行。
4.3	4.3（6.260054）

注：前出の表に記載された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アプライアンスでは、管理者はCisco IMCを前出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）ユーザーガイド』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	最初の修正済みファームウェアリリース	修復方法
Cisco Telemetry Broker アプライアンス	6.0(2.260143)[1]	ファームウェアアップデートCTB-FIRMWARE-6.0.2.260143-M6.isoをインストールします。
IEC6400 エッジ コンピューティング アプライアンス	4.3（6.260054）	IEC6400-HUU-4.3.6-260054.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(2.260020)(M5) 4.3(6.260054)(M6)	TechNoteに記載されている手順に従ってください。
Secure Firewall Management(FMC)Centerアプライアンス	4.3(2.260020)(M5) 6.0(2.260143)[1](M6)	ホットフィックスGAを適用します。
Cisco Secure Malware Analytics アプライアンス	4.3(2.260020)(M5) 4.3(6.260054)(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	最初の修正済みファームウェアリリース	修復方法
Cisco Secure Network Analytics アプライアンス	4.3(2.260020)(M5) 6.0(2.260143)[1](M6)	M5に対して、ファームウェアアップデートpatch-common-SNA-FIRMWARE-4.3.2.260020-M5-v2-01.swuをインストールします。 M6の場合、ファームウェアアップデートpatch-common-SNA-FIRMWARE-6.0.2260143-M6-v2-01.swuをインストールします。
Secure Network Server(ISE SNS)アプライアンス	4.3(2.260020)(M5) 6.0(2.260143)[1](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。

1. 修正済みの6.0(2.260143)ファームウェアリリースには、Cisco IMC 6.0(2.260094)パッケージリリースが含まれています。この修正済みリリースにアップグレードすると、Cisco IMC UI Dashboardページの Firmware Versionに6.0(2.260094)が表示されます。 Administration > Firmware Managementの下の Last HSU bundle usedフィールドに、修正済みの6.0(2.260143)リリースが表示されます。

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

この脆弱性を報告していただいたポーランドのING Hubs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-xss-7EhBFxBp

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8月5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。