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-A2tkgVAB
初公開日 : 2026-04-01 16:00
バージョン 1.0 : Final
CVSSスコア : 6.1
回避策 : No workarounds available
Cisco バグ ID : CSCws07240 CSCwr60948 CSCws07351 CSCws07154 CSCwr60939 CSCwr60943 CSCws07585 CSCws07596 CSCwr60933 CSCwr60944 CSCws07597 CSCws07159 CSCws07591 CSCws07501 CSCws07589 CSCwr60930 CSCws07239

CVE-2026-20085
CVE-2026-20090
CVE-2026-20088
CVE-2026-20089
CVE-2026-20087

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、リモート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-xss-A2tkgVAB

該当製品

脆弱性のある製品

公開時点で、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した。

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-2026-20085 CVE-2026-20087 CVE-2026-20088 CVE-2026-20089 CVE-2026-20090	CSCws07159 CSCws07240、 CSCws07501 CSCws07585 CSCws07591 CSCws07597
Catalyst 8300 シリーズ エッジ uCPE	CVE-2026-20085 CVE-2026-20087 CVE-2026-20089 CVE-2026-20090	CSCws07154 CSCws07239、 CSCws07351 CSCws07589 CSCws07596
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-2026-20085 CVE-2026-20087 CVE-2026-20088 CVE-2026-20089 CVE-2026-20090	CSCwr60930 CSCwr60933、 CSCwr60939 CSCwr60943 CSCwr60944 CSCwr60948
UCS E シリーズ サーバー M3	CVE-2026-20085 CVE-2026-20087 CVE-2026-20088 CVE-2026-20089 CVE-2026-20090	CSCws07159 CSCws07240、 CSCws07501 CSCws07585 CSCws07591 CSCws07597
UCS EシリーズサーバM6	CVE-2026-20085 CVE-2026-20087 CVE-2026-20089 CVE-2026-20090	CSCws07154 CSCws07239、 CSCws07351 CSCws07589 CSCws07596
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-2026-20087 CVE-2026-20089 CVE-2026-20090	CSCwr60933、 CSCwr60939 CSCwr60944 CSCwr60948

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。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(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

このアドバイザリの公開時点で脆弱性が存在するシスコ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。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。

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-2026-20085がCisco UCS Sシリーズストレージサーバに影響を与えないことを確認しました。

シスコは、CVE-2026-20087、CVE-2026-20089、およびCVE-2026-20090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搭載したCisco UCS Sシリーズストレージサーバには影響を与えないことを確認しました。

シスコは、CVE-2026-20088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。

- Catalyst 8300 シリーズ エッジ uCPE
- UCS Eシリーズサーバ M6
- 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-2026-20085:Cisco IMCのReflected XSS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、認証されていない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リフレクト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。

バグID: CSCwr60930、CSCws07154、CSCws07159
CVE ID：CVE-2026-20085
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6.1
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVE-2026-20087、CVE-2026-20088、CVE-2026-20089、およびCVE-2026-20090:Cisco IMCによって蓄積されたXSS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4つの脆弱性により、管理者権限を持つ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ストアドXSS攻撃を実行できる可能性があります。

これらの脆弱性は、ユーザ入力の不十分な検証に起因します。攻撃者は、細工されたリンクを該当インターフェイスのユーザにクリックさせるように仕向けることで、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: CSCwr60933、CSCws07239、CSCws07240、CSCwr60939、CSCws07351、CSCws07501、CSCwr60943、CSCws075 5、CSCwr60944、CSCws07589、CSCws07591、CSCwr60948、CSCws07596、CSCws07597
CVE ID: CVE-2026-20087、CVE-2026-20088、CVE-2026-20089、CVE-2026-20090
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.8
CVSS ベクトル：CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/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

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。

左の列にはシスコソフトウェアリリースが、右の列にはリリースがこのアドバイザリに記載された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リリースが示され

ています。

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。
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	4.3(2.260007)(M5)	『Cisco Secure Network Server 3600シリーズ

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
Server アプライアンス	4.3(6.260017)(M6) 6.0(2.260044)(M6)	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 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-A2tkgVAB

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

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。