Cisco Integrated Management Controller における引数インジェクションの脆弱性

アドバイザリーID : cisco-sa-cimc-arg-inject-upSHdMfU
初公開日 : 2026-08-05 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 : CSCwu57141 CSCwu57142 CSCwt16342 CSCwt45063

CVE-2026-20200
CVE-2026-20288

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-arg-inject-upSHdMfU

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以下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	CVE-2026-20288	CSCwu57141

製品	CVE ID	Cisco Bug ID
ステム（ENCS）		
Catalyst 8300 シリーズ エッジ uCPE	CVE-2026-20288	CSCwu57142
スタンドアロンモードの Cisco UCS C シリーズ M5 および M6 ラックサーバー	CVE-2026-20288	CSCwt45063
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	CVE-2026-20200 CVE-2026-20288	CSCwt16342 CSCwt45063
UCS E シリーズ サーバー M3	CVE-2026-20288	CSCwu57141
UCS E シリーズ M6 サーバー	CVE-2026-20288	CSCwu57142
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	CVE-2026-20288	CSCwt45063

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
- 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

シスコは、次のシスコ製品がCVE-2026-20200で説明されている脆弱性の影響を受けないことを確認しました。

- 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）
- 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 および M6 ラックサーバー
- UCS EシリーズM3およびM6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

詳細

これらの脆弱性は互いに依存関係がありません。いずれかの脆弱性をエクスプロイトするために、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受ける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-2026-20200：Cisco IMC における引数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存在する脆弱性により、権限の低い認証された

リモートの攻撃者が、該当する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マンドを実行し、root に権限の昇格を行う可能性があります。

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、巧妙に細工された入力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行うことにより、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、攻撃者は基盤となるオペレーティングシステムで root ユーザーとして任意のコマンドを実行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。

バグ ID：CSCwt16342
CVE ID：CVE-2026-20200
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-2026-20288：Cisco IMC における引数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存在する脆弱性により、管理者権限を持つ認証されたリモートの攻撃者が、該当する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マンドを実行し、root に権限の昇格を行う可能性があります。

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、巧妙に細工された入力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行うことにより、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、攻撃者は基盤となるオペレーティングシステムで root ユーザーとして任意のコマンドを実行できるようになります。

攻撃者が root ユーザーになると、新たなセキュリティへの影響が生じる可能性があります。そのため、シスコは、この脆弱性に SIR のスコアとして「中」ではなく「高」を割り当てました。

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：CSCwt45063、CSCwu57141、および CSCwu57142
CVE ID：CVE-2026-20288
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の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	CVE-2026-20288 の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	CVE-2026-20288 の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	CVE-2026-20288 の最初の修正済みリリース
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	CVE-2026-20288 の最初の修正済みリリース
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]

UCS C シリーズ M7 および M8 ラックサーバー

Cisco UCS サーバー ソフトウェア リリース	CVE-2026-20200 の最初の修正済みリリース	CVE-2026-20288 の最初の修正済みリリース
4.3 より前	修正済みリリースに移行。	修正済みリリースに移行。
4.3	4.3 (6.260033)	4.3 (6.260054)
6.0	6.0 (2.260044)	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) の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 の [ダッシュボード (Dashboard)] ページの [ファームウェアバージョン (Firmware Version)] の下に 6.0(2.260094) と表示されます。[管理 (Administration)] > [ファームウェア管理 (Firmware Management)] の下の [最後に使用されたHSUバンドル (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	CVE-2026-20288 の最初の修正済みリリース
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	CVE-2026-20288 の最初の修正済みリリース
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	CVE-2026-20288 の最初の修正済みリリース
4.3 より前	修正済みリリースに移行。
4.3	4.3 (6.260054)

注： 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]	ファームウェアの更新 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 IOS XRv 9000 M7 アプライアンス	6.0(2.260143)[1]	IOS XR 26.3.1 (2026 年 8 月) にアップグレードし、IOS XR CLI からアプライアンス ファームウェアをアップグレードします。
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います。
Secure Firewall Management (FMC) Center アプライアンス	4.3(2.260020) (M5) 6.0(2.260143)[1] (M6、M8)	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。
Cisco Secure Network Analytics アプライアンス	4.3(2.260020) (M5) 6.0(2.260143)[1] (M6)	M5 の場合、ファームウェアの更新 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、ファームウェアの更新 patch-

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
		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、M8)	Cisco Secure Network Server 3600 シリーズ、Cisco Secure Network Server 3700 シリーズ、または Cisco Secure Network Server 3800 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) の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 の [ダッシュボード（Dashboard）] ページの [ファームウェアバージョン（Firmware Version）] の下に 6.0(2.260094) と表示されます。[管理（Administration）] > [ファームウェア管理（Firmware Management）] の下の [最後に使用されたHSUバンドル（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 は、CVE-2026-20200 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。

Cisco PSIRT では、このアドバイザリに記載されている脆弱性のいかなる悪用も認識していません。

出典

CVE-2026-20200 を報告してくださった NSIDE ATTACK LOGIC GmbH 社の Christoph Peil 氏に感謝いたします。

CVE-2026-20288 は、内部セキュリティテスト中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-arg-inject-upSHdMfU

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

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。