# Cisco Integrated Management Controller認証バイパスの脆弱性


アドバイザリーID : cisco-sa-cimc-auth-bypass-AgG2BxTn
初公開日 : 2026-04-01 16:00
バージョン 1.0 : Final
CVSSスコア : 9.8
回避策 : No workarounds available
Cisco バグ ID : CSCwq68912 CSCwq55648 CSCwq55659

CVE-2026-20093

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)のパスワード変更機能の脆弱性により、認証されていないリモートの攻撃者が認証をバイパスし、Adminとしてシステムにアクセスできる可能性があります。

この脆弱性は、パスワード変更要求の不適切な処理に起因します。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、攻撃者は認証をバイパスし、管理者ユーザを含むシステム上の任意のユーザのパスワードを変更して、そのユーザとしてシステムへのアクセスを取得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。

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-auth-bypass-AgG2BxTn

## 該当製品

### 脆弱性のある製品

この脆弱性は、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。

- 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)(CSCwq55648)
- Catalyst 8300シリーズEdge uCPE(CSCwq68912)
- 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(CSCwq55659)
- UCS EシリーズサーバM3(CSCwq55648)
- UCS EシリーズサーバM6(CSCwq68912)

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
- 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

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 S シリーズ ストレージ サーバ
- UCS Xシリーズモジュラシステム
- 統合されたエッジ

## 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。

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 | Cisco 5000シリーズENCSの最初の修正済みリリース |
|---|---|
| 4.15 以前 | 4.15.5 |

| Cisco NFVIS リリース | Cisco Catalyst 8300シリーズエッジuCPEの最初の修正済みリリース |
|---|---|
| 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（1.250174） |

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 |

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(1.250192)(M6) | ファームウェアアップデートm6-tb2300-ctb-firmware-6.0-1.250192.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 | 4.3(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)<br>4.3(6.260017)(M6) | リリース4.2.5以降にアップグレードし、『TechNote』の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)<br>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)<br>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)<br>6.0(1.250192)(M6) | M5に対して、patch-common-SNA-FIRMWARE-20260210-M5-REL.isoをインストールします。<br>M6の場合、patch-common-SNA-FIRMWARE-20260210-M6-REL.isoをインストールします。 |
| Cisco Secure Network Server アプライアンス | 4.3(2.260007)(M5)<br>4.3(6.260017)(M6)<br>6.0(1.250174)(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セキュリティ研究者jyhに感謝いたします。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn

## 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。