

Cisco UCS Managerソフトウェアの権限昇格の脆弱性



アドバイザリーID : cisco-sa-ucsm-afwae- [CVE-2026-](#)

mOgUfyLn

[20037](#)

初公開日 : 2026-02-25 16:00

バージョン 1.0 : Final

CVSSスコア : [4.4](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwm68934](#)

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 UCS ManagerソフトウェアのNX-OS CLI特権レベルの脆弱性により、読み取り専用権限を持つ認証されたローカルの攻撃者が、該当システムでファイルを変更し、不正な操作を実行できる可能性があります。

この脆弱性は、不要な特権がユーザに与えられるために存在します。攻撃者は、読み取り専用ユーザとしてデバイスに認証され、NX-OS CLIに接続することで、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、攻撃者はファイルシステム内でファイルを作成または上書きしたり、該当デバイスで限られた特権アクションを実行したりできます。

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。

このアドバイザリーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-afwae-mOgUfyLn>

このアドバイザリーは、2026年2月に公開されたCisco FXOSおよびNX-OSソフトウェアセキュリティアドバイザリーバンドルの一部です。アドバイザリーとリンクの一覧については、『[Cisco Event Response: February 2026 Semiannual Cisco FXOS and NX-OS Software Security Advisory Bundled Publication](#)』を参照してください。

該当製品

脆弱性のある製品

公開時点では、デバイス設定に関係なく、脆弱性のあるCisco UCS Managerソフトウェアリリースを実行する次のシスコ製品がこの脆弱性の影響を受けました。

- UCS 6400 シリーズ ファブリック インターコネクト
- UCS 6500 シリーズ ファブリック インターコネクト
- UCS Xシリーズダイレクトファブリックインターコネクト9108 100G

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。このアドバイザリの先頭にあるバグIDの詳細情報のセクションで、最新の情報を確認してください。

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、この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。

- Firepower 1000 シリーズ
- Firepower 2100 シリーズ
- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス
- MDS 9000 シリーズ マルチレイヤ スイッチ
- Nexus 3000 シリーズ スイッチ
- Nexus 5500 プラットフォーム スイッチ
- Nexus 5600 プラットフォーム スイッチ
- Nexus 6000 シリーズ スイッチ
- Nexus 7000 シリーズ スイッチ
- ACI モードの Nexus 9000 シリーズ ファブリック スイッチ
- スタンドアロン NX-OS モードの Nexus 9000 シリーズ スイッチ
- Cisco Secure Firewall 200 シリーズ
- Cisco Secure Firewall 1200 シリーズ
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- Cisco Secure Firewall 6100 シリーズ
- UCS 6300 シリーズ ファブリック インターコネクト
- UCS 6600 シリーズ ファブリック インターコネクト

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。

Cisco UCS ソフトウェア

発行時点では、次の表に示すリリース情報は正確でした。このアドバイザリの手前にあるバグ IDの詳細情報のセクションで、最新の情報を確認してください。

左の列はシスコソフトウェアリリースを、右の列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、およびこの脆弱性に対する修正を含むリリースを示しています。

UCS 6400シリーズ、6500シリーズ、および9108 100Gファブリックインターコネク

Cisco UCS 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)
4.1 以前	修正済みリリースに移行。
4.2	修正済みリリースに移行。
4.3	4.3(6f)
6.0	脆弱性なし

Cisco UCS ソフトウェアに最適なリリースを確認するには、デバイスのリリースノートに記載されている推奨リリースに関するドキュメントを参照してください。

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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-afwae-mOgUfyLn>

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2月25日

利用規約

本アドバイザー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。本アドバイザー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。

本アドバイザーの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、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。