Cisco UCS Managerソフトウェアのコマンドインジェクションの脆弱性

アドバイザリーID : cisco-sa-ucs-multi-cmdinj-E4Ukjyrz
初公開日 : 2025-08-27 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwn06825 CSCwm88176

CVE-2025-20294
CVE-2025-20295

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CLIおよび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、管理権限を持つ認証された攻撃者が、該当システムでコマンドインジェクション攻撃を実行し、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-ucs-multi-cmdinj-E4Ukjyrz

このアドバイザリは、2025年8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バンドルの一部です。これらのアドバイザリとリンクの一覧については、『シスコイベントレスポンス：Cisco FXOSおよびNX-OSソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年8月）』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、これらの脆弱性は、デバイス設定に関係なく、Cisco UCS Managerソフトウェア

を実行している次のシスコ製品に影響を与えました。

- UCS 6300 シリーズ ファブリック インターコネクト
- 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。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、これらの脆弱性が次のシスコ製品に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
- VMware vSphere 向け Nexus 1000 Virtual Edge
- 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 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ

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-2025-20294:Cisco UCS Managerソフトウェアのコマンドインジェクションの脆弱性

Cisco UCS ManagerソフトウェアのCLIおよび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、管理権限を持つ認証されたリモートの攻撃者が、該当システムでコマンドインジェクション攻撃を実行し、権限を rootに昇格させる可能性があります。

これらの脆弱性は、ユーザが指定するコマンド引数の入力検証が不十分であることに起因します。攻撃者は、デバイスに認証され、巧妙に細工された入力を該当コマンドに送信することで、これら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rootレベルの権限を使用して、該当デバイスの基盤となるオペレーティングシステム上で任意のコマンドを実行でき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: CSCwn06825
CVE ID：CVE-2025-20294
セキュリティ影響評価（SIR）：中
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

CVE-2025-20295:Cisco UCS Managerソフトウェアのコマンドインジェクションの脆弱性

Cisco UCS ManagerソフトウェアのCLIにおける脆弱性により、管理者権限を持つ認証されたローカルの攻撃者が、該当デバイスの基盤となるオペレーティングシステムのファイルシステム上で、システムファイルを含む任意のファイルの読み取りや作成、またはファイルの上書きを行う可能性があります。

この脆弱性は、ユーザが指定するコマンド引数の不十分な入力検証に起因します。攻撃者は、デバイスに認証され、巧妙に細工された入力を該当コマンドに送信することで、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、該当デバイスの基盤となるオペレーティングシステムのファイルシステム上で、システムファイルを含む任意のファイルを読み取りや作成、または上書きできるようになります。この脆弱性を不正利用するには、攻撃者は該当デバイスで有効な管理者クレデンシャルを持っている必要があります。

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: CSCwm88176
CVE ID：CVE-2025-20295
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：6
CVSSベクトル：CVSS:3.1/AV:L/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

ソフトウェアのアップグレードを検討する際には、シスコ セキュリティ アドバイザリ ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

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。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。

UCS 6300シリーズ、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ト

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	4.2(3p)
4.3	4.3(6c)
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とその公表は確認しておりません。

出典

この脆弱性は、シスコ内部でのシステム 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-ucs-multi-cmdinj-E4Ukjyrz

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	2025年8月27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。