Cisco NX-OSソフトウェアのコマンドインジェクションの脆弱性

Medium

アドバイザリーID : cisco-sa-nxos-cmdinj-qhNze5Ss　CVE-2025-20292
初公開日 : 2025-08-27 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 : CSCwn39957 CSCwn39955 CSCwn39958 CSCwm88173 CSCwo71696 CSCwn39942 CSCwn39953

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 NX-OSソフトウェアのCLIにおける脆弱性により、認証されたローカル攻撃者が、該当デバイスの基盤となるオペレーティングシステムに対してコマンドインジェクション攻撃を実行する可能性があります。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ユーザクレデンシャルを持っている必要があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、該当CLIコマンドの引数として巧妙に細工された入力を入力することにより、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、ルート以外のユーザアカウントの権限を使用して、基盤となるオペレーティングシステム上でファイルの読み取りおよび書き込みを行えるようになります。ファイルシステムアクセスは、その非ルートユーザアカウントに付与された権限に制限されます。

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-nxos-cmdinj-qhNze5Ss

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

公開時点では、この脆弱性はデバイス設定に関係なく、次のシスコ製品に影響を与えていました。

- MDS 9000シリーズマルチレイヤスイッチ(CSCwn39942)
- VMware vSphere向けNexus 1000 Virtual Edge(CSCwo71696)
- Nexus 3000シリーズスイッチ(CSCwn39953)
- Nexus 5500プラットフォームスイッチ(CSCwn39958)
- Nexus 5600プラットフォームスイッチ(CSCwn39958)
- Nexus 6000シリーズスイッチ(CSCwn39958)
- Nexus 7000シリーズスイッチ(CSCwn39955)
- ACIモードのNexus 9000シリーズファブリックスイッチ(CSCwn39957)
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ(CSCwn39953)
- UCS 6400シリーズファブリックインターコネクト(CSCwm88173)
- UCS 6500シリーズファブリックインターコネクト(CSCwm88173)
- 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(CSCwm88173)

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
- Cisco Secure Firewall 3100 シリーズ
- Cisco Secure Firewall 4200 シリーズ
- UCS 6300 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

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 NX-OS ソフトウェア

お客様が Cisco NX-OS ソフトウェアの脆弱性による侵害の可能性を判断できるように、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース（「First Fixed」）を特定できます。 また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース（「Combined First Fixed」）を特定できます。

このツールを使用するには、「Cisco Software Checker」ページの手順に従います。または、次のフォームを使用して、特定のソフトウェアリリースに影響を及ぼす脆弱性を検索します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、セキュリティ影響評価（SIR）が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. 該当するソフトウェアを選択します。
3. 該当するプラットフォームを選択します。
4. リリース番号を入力します。たとえば、Cisco Nexus 3000シリーズスイッチの場合は10.4(4)、ACIモードのCisco NX-OSソフトウェアの場合は16.0(8e)などです。
5. [チェック（Check）] をクリックします。

2		Critical,High,Medium
このアドバイザのみ	Cisco NX-OS ソフトウェア	
あらゆるプラットフォーム		
Enter release number	Check	

Cisco UCS ソフトウェア

公開時点では、次の表のリリース情報は正確でした。最新の完全な情報については、このアドバイザリの先頭にあるバグIDの詳細を参照してください。

左の列にはシスコのソフトウェアリリースが、中央の列と右の列には、その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が示されています。

UCS 6400および6500シリーズ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	UCS Managerモードの最初の修正済みリリース	Intersightマネージドモードの最初の修正済みリリース
4.1 以前	修正済みリリースに移行。	修正済みリリースに移行。
4.2	4.2(3p)	4.2(3p)
4.3	4.3 (6a)	4.3 (6.250048)
6.0	脆弱性なし	脆弱性なし

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

Cisco UCS ソフトウェアリリース	UCS Managerモードの最初の修正済みリリース	Intersightマネージドモードの最初の修正済みリリース
4.3	4.3 (6a)	4.3 (6.250094)
6.0	脆弱性なし	脆弱性なし

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。

関連情報

Cisco Nexus スイッチに最適な Cisco NX-OS ソフトウェアリリースの決定に際してサポートが必要な場合は、以下の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。セキュリティ アドバイザリでより新しいリリースが推奨されている場合は、そのアドバイザリのガイダンスに従うことをお勧めします。

Cisco MDS シリーズ スイッチ
Cisco Nexus 3000 Series Switches
Cisco Nexus 5500 プラットフォーム スイッチ
Cisco Nexus 5600 プラットフォームスイッチ
Cisco Nexus 6000 Series Switches
Cisco Nexus 7000 Series Switches

Cisco Nexus 9000 Series Switches
ACI モードの Cisco Nexus 9000 シリーズ スイッチ

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。

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-nxos-cmdinj-qhNze5Ss

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。