

Cisco Nexus 3000および9000シリーズスイッチ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-nxos-ici-

dpOjbWxk

初公開日 : 2025-02-26 16:00

バージョン 1.0 : Final

CVSSスコア : [5.1](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwm09739](#)

[CVE-2025-](#)

[20161](#)

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

スタンドアロンNX-OSモードのCisco Nexus 3000シリーズスイッチおよびCisco Nexus 9000シリーズスイッチのソフトウェアアップグレードプロセスにおける脆弱性により、有効な管理者クレデンシャルを持つ認証されていない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。

この脆弱性は、ソフトウェアイメージ内の特定の要素の検証が不十分であることに起因します。攻撃者は、巧妙に細工されたイメージをインストールすることにより、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root権限を使用して、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できる可能性があります。

注：管理者はインストールの前に、すべてのソフトウェアイメージのハッシュを検証する必要があります。

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。

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-nxos-ici-dpOjbWxk>

このアドバイザリーは、2025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。これらのアドバイザリー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ー公開資料（半年刊、2025年2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、デバイスの設定にかかわらず、この脆弱性はスタンドアロンNX-OSモードのCisco Nexus 3000シリーズスイッチおよびCisco Nexus 9000シリーズスイッチに影響を与えていました。

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、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
- VMware vSphere 向け Nexus 1000 Virtual Edge
- 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
- 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
- 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

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問題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 7.0(3)I7(5)、ACIモードのCisco NX-OSソフトウェアの場合は14.0(1h)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	

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 Product Security Incident Response Team (PSIRT) 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を確認していません。

出典

この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のStephen Kubikによる内部セキュリティテストで発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ici-dpOjbWxk>

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2月26日

利用規約

本アドバイザリ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。本アドバイザリ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。

本アドバイザリ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。