

Cisco NX-OSソフトウェアのCLIにおける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-cli- [CVE-2023-20050](#)
cmdinject-euQVK9u
初公開日 : 2023-02-22 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 : [CSCwd18012](#)
[CSCwd18013](#) [CSCwd18011](#)
[CSCwd00653](#) [CSCwd18009](#)

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 システムで任意のコマンドを実行できるようになります。

この脆弱性は、特定のCLIコマンドに渡される引数の検証が不十分であることに起因します。攻撃者は、該当コマンドの引数として巧妙に細工された入力を含めることによって、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、攻撃者は現在ログインしているユーザの権限を使用して、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-cli-cmdinject-euQVK9u>

このアドバイザリーは、2023年2月の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公開の一部です。アドバイザリーの完全なリストとそのリンクについては、『[Cisco Event Response: February 2023 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

この脆弱性は、Cisco NX-OSソフトウェアの脆弱性が存在するリリースを実行している次のシスコ製品に影響を与えました。

- MDS 9000シリーズマルチレイヤスイッチ([CSCwd18009](#))
- Nexus 1000 Virtual Edge for VMware vSphere([CSCwd18012](#))
- Microsoft Hyper-V向けNexus 1000Vスイッチ([CSCwd18012](#))
- VMware vSphere向けNexus 1000Vスイッチ([CSCwd18012](#))
- Nexus 3000シリーズスイッチ([CSCwd00653](#))
- Nexus 5500プラットフォームスイッチ([CSCwd18013](#))
- Nexus 5600プラットフォームスイッチ([CSCwd18013](#))
- Nexus 6000シリーズスイッチ([CSCwd18013](#))
- Nexus 7000シリーズスイッチ([CSCwd18011](#))
- スタンドアロンNX-OSモードのNexus 9000シリーズスイッチ([CSCwd00653](#))

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記載されている製品のみが、こ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
- 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
- UCS 6200 シリーズ ファブリック インターコネクト
- 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アップグレードソリューション一式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 IOS 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 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)と入力します。
5. [チェック (Check)] をクリックします。

Cisco Nexus 3000、7000、および 9000 シリーズ スイッチの SMU

シスコはこの脆弱性に対処する次の SMU もリリースしています。次の SMU を Cisco.com の [Software Center](#) からダウンロードできます。

[Cisco NX-OS ソフト]	[Platform	[SMU 名
-------------------	-----------	--------

ウェアリリース		
8.2(9)	Nexus 7000 シリーズ ス イッチ	n7000-s2-dk9.8.2.9.CSCwd18011.bin n7700-s2-dk9.8.2.9.CSCwd18011.bin
9.3(10)	Nexus 3000 および 9000 シリーズ ス イッチ	nxos.CSCwd00653-n9k_ALL-1.0.0-9.3.10.lib32_n9000.rpm
10.2(4)	Nexus 3000 および 9000 シリーズ ス イッチ	nxos64-cs.CSCwd00653-1.0.0-10.2.4.lib32_64_n9000.rpm nxos64-msll.CSCwd00653-1.0.0-10.2.4.lib32_64_n9000.rpm

Cisco Nexus 3000、7000、および9000シリーズスイッチ用Cisco NX-OSソフトウェアでのSMUのダウンロードとインストールの詳細については、[Cisco Nexus 3000シリーズスイッチ](#)、[Cisco Nexus 7000シリーズスイッチ](#)、および[Cisco Nexus 9000シリーズスイッチ用Cisco NX-OSシステム管理設定ガイド](#)の「ソフトウェアメンテナンスアップグレードの実行」セクションを参照してください。

その他のリソース

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](#)

[VMware 向け Cisco Nexus 1000V 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

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-cli-cmdinject-euQVK9u>

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	2023年2月22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。