Cisco Firepower 4100シリーズ、Firepower 9300セキュリティアプライアンス、およびUCSファブリックインターコネクト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-nxfp-cmdinj-XXBZjtR **初公開日 :** 2023-02-22 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.0 **回避策 :** No workarounds available **Cisco バグ ID :** CSCwd11206 CSCwd11228 CSCwc52151	CVE-2023-20015

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 Firepower 4100シリーズ、Cisco Firepower 9300セキュリティアプライアンス、およびCisco UCS 6200、6300、6400、および6500シリーズファブリックインターコネクトのCLIの脆弱性により、認証されたローカルの攻撃者が不正なコマンドを挿入する可能性があります。

この脆弱性は、ユーザが提供するコマンド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CLI内で不正なコマンドを実行できる可能性があります。*Administrator*権限を持つ攻撃者は、*root*レベル権限を持つCisco UCS 6400および6500シリーズファブリックインターコネクト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する可能性もあります。

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-nxfp-cmdinj-XXBZjtR

このアドバイザリは、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

ザリバンドル公開の一部です。アドバイザリ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 FXOSまたは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。

- Firepower 4100 シリーズ
- Firepower 9300 セキュリティ アプライアンス
- 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

注：Cisco UCS 6400および6500シリーズファブリックインターコネクトでのみ、*Administrator*権限を持つユーザが*root*レベル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コマンドを実行できます。影響を受ける他の製品では影響が少なく、低特権ユーザがCLI内で実行される一部の許可されていない非特権コマンドにアクセスすることしかできず、基盤となるオペレーティングシステムではアクセスできません。

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
- 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 1000V Switch for Microsoft Hyper-V
- Nexus 1000V Switch for VMware vSphere
- 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

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 FXOS および NX-OS ソフトウェア

お客様が Cisco FXOS および 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 Firepower 4100シリーズセキュリティアプライアンスの場合は**2.9.1.158**、Cisco Nexus 3000シリーズスイッチの場合は**7.0(3)I7(5)**などです。
5. [チェック（Check）] をクリックします。

Cisco UCS ソフトウェア

発行時点では、次の表に記載されている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。

左の列はシスコソフトウェアリリースを示し、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ます。

UCS 6200、6300、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	First Fixed Release (修正された最初のリリース)
4.0 より前	修正済みリリースに移行。
4.0	4.0(4o)
4.1	4.1(3k)
4.2	4.2(2d)

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された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

この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のMichael Hegglin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-nxfp-cmdinj-XXBZjtR

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、単独の転載や意訳を施した場合、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。