Cisco NX-OS システム ソフトウェア パッチ インストール コマンド インジェクト脆弱性

Medium	**アドバイザリーID :** cisco-sa-20171129-nxos8 **初公開日 :** 2017-11-29 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 6.7 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvg04072 CSCvf23735	CVE-2017-12341

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 システム ソフトウェアの CLI の脆弱性はコマンド インジェクト 攻撃を行う認証された、ローカル攻撃者を可能にする可能性があります。 攻撃者は有効な管理者の資格情報がこのエクスプロイトを行うことを必要とします。

脆弱性はソフトウェアパッチのインストール時に不十分な入力の検証が原因です。 攻撃者はパッチ アクティベーション前に発生する脆弱 な オペレーションを用いる巧妙に細工されたパッチ イメージのインストールによってこの脆弱性を不正利用する可能性があります。 エクスプロイトは攻撃者が *ルート*として影響を受けたシステムの任意のコマンドを実行することを可能にする可能性があります。

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-nxos8

該当製品

脆弱性のある製品

この脆弱性は Cisco NX-OS システム ソフトウェアを実行する以下の製品に影響を及ぼします:

- マルチレイヤ ディレクタ スイッチ
- Nexus 2000 シリーズ ファブリック エクステンダ

- Nexus 5000 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
- Nexus 7700 シリーズ スイッチ
- Unified Computing System マネージャ

該当するリリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

脆弱性を含んでいないことが確認された製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

Cisco は以下の製品がこの脆弱性から影響を受けないことを確認しました:

- Firepower 2100 シリーズ
- Firepower 4100 シリーズ次世代ファイアウォール
- Firepower 9300 セキュリティ アプライアンス
- Nexus 1000V シリーズ スイッチ
- Nexus 3000 シリーズ スイッチ
- Nexus 3500 プラットフォーム スイッチ
- シスコ アプリケーション セントリック インフラストラクチャ（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
- Nexus 9500 R シリーズ ラインカードおよびファブリック モジュール

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

修正済みソフトウェアリリースについての情報に関しては、このアドバイザリの上で Cisco バグ ID を参照して下さい。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts 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。

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-nxos8

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017-November-29

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。