Cisco Nexus シリーズ スイッチ CLI 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-nss **初公開日 :** 2017-11-29 16:00 **最終更新日 :** 2018-01-11 18:32 **バージョン 1.1 :** Final **CVSSスコア :** 6.3 **回避策 :** No workarounds available **Cisco バグ ID :** CSCve99902 CSCvf14879	CVE-2017-12330

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 インジェクト不正侵入を行う認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性は CLI パーサーがコマンド ライン引数の不十分な入力の検証が原因です。 攻撃者は巧妙に細工されたコマンド引数を脆弱な CLI コマンドにインジェクトし、デバイスの基礎オペレーティング システムに不正アクセスを得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。 エクスプロイトは攻撃者がユーザの特権レベルで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。 複数の仮想デバイス コンテキスト（VDC）をサポートする製品で、この脆弱性は攻撃者がユーザー環境の外部のユーザの特権レベルで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-nss

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シスコ製品に影響を及ぼ

します:

脆弱なプロダクト	Cisco Bug ID
MDS 9000 シリーズ マルチレイヤ スイッチ	CSCve99902
Nexus 2000 年、5000、5500、5600、および 6000 シリーズ スイッチ	CSCvf14879
Nexus 3000 シリーズ スイッチ	CSCve99902
Nexus 7000 および 7700 シリーズ スイッチ	CSCve99902
Nexus 9000 シリーズ スイッチ-スタンドアロン、NX-OS モード	CSCve99902
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	CSCve99902

該当するリリースについての情報に関しては、上記の表におよびこの状況報告の上にリストされている 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。

シスコは、この脆弱性が以下の製品には影響を与え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 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
- Unified Computing System マネージャ

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、この状況報告の上で 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-nss

改訂履歴

Version	Description	Section	Status	日付
1.1	該当製品の表および各々の影響を受けた製品のためのバグID を追加しました。	脆弱性のある製品	Final	2018-January-11
1.0	初回公開リリース		Final	2017 年 11 月 29 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。