Cisco マルチレイヤディレクター、Nexus 7000 シリーズおよび Nexus 7700 シリーズはスイッチ シェル 不正アクセス脆弱性を強くぶつけます

Medium	**アドバイザリーID :** cisco-sa-20171129-switch **初公開日 :** 2017-11-29 16:00 **バージョン 1.0 :** Final **CVSSスコア :** 4.2 **回避策 :** No workarounds available **Cisco バグ ID :** CSCvd86513	CVE-2017-12340

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

MDS マルチレイヤディレクター スイッチ、Cisco Nexus 7000 シリーズ スイッチおよび Cisco Nexus 7700 シリーズ スイッチを on Cisco 実行する Cisco NX-OS システム ソフトウェアの脆弱性は Bash シェルがシステムでディセーブルにされても影響を受けたデバイスのオペレーティング システムの Bash シェルにアクセスする認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性は影響を受けたシステムの大蛇スクリプトを書くサンドボックスのある特定の機能に通じるユーザが指定するパラメータの不十分な sanitization が原因です。 攻撃者はスクリプトを書くサンドボックスをエスケープし、影響を受けたシステムのための認証済みユーザの特権のオペレーティング システムの Bash シェルを入力するのにこの脆弱性を不正利用する可能性があります。 この脆弱性を不正利用するために、攻撃者は影響を受けたシステムにローカルアクセスをアクセスできるおよび管理上または大蛇実行特権の影響を受けたシステムに認証する必要があります。

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-switch

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 ソフトウェアの脆弱なリリースを実行する場合以下のシスコ製品に影響を及ぼします:

- MDS マルチレイヤディレクター スイッチ
- Nexus 7000 シリーズ スイッチ
- Nexus 7700 シリーズ スイッチ

該当するソフトウェア 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。

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シスコ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 次世代ファイアウォール（NGFW）
- Firepower 4100 シリーズ 次世代ファイアウォール（NGFW）
- 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 2000 シリーズ ファブリック エクステンダ
- Nexus 3000 シリーズ スイッチ
- Nexus 3500 プラットフォーム スイッチ
- 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
- 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
- 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-switch

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

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。