Cisco NX-OS ソフトウェア大蛇パーサー エスケープ脆弱性

Medium	**アドバイザリーID :** cisco-sa-20171018-ppe **初公開日 :** 2017-10-18 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 :** CSCvd86490 CSCvf12804 CSCvf12815 CSCvd86484 CSCvf15198 CSCvb86832 CSCvf12757 CSCvd86474 CSCvd86479 CSCve97102	CVE-2017-12301

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 ソフトウェアの大蛇スクリプトを書くサブシステムの脆弱性は大蛇パーサーをエスケープし、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。

ある特定の大蛇に通じるユーザが指定するパラメータの不十分な sanitization による脆弱性存在は影響を受けたデバイスのスクリプトを書くサンドボックスの内で機能します。 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、認証済みユーザの特権の基礎オペレーティング システムの任意のコマンドを実行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目標とされたデバイスに認証する必要があります。 これらの必要条件は正常なエクスプロイトの可能性を制限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-20171018-ppe

該当製品

脆弱性のある製品

この脆弱性は Cisco NX-OS ソフトウェアを実行する場合以下のシスコ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 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
Nexus 7000 シリーズ スイッチ
Nexus 7700 シリーズ スイッチ
Nexus 9000 シリーズ スイッチ-スタンドアロン、NX-OS モード
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

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、この状況報告の上で 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
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 9000 シリーズ ファブリックスイッチ- ACI モード
Unified Computing System マネージャ

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。

回避策

この脆弱性に対処する回避策はありません。 ただし、管理者は非常に信頼されたユーザだけ大蛇サンドボックスへのアクセスを許可されるようにすることによってこの脆弱性への公開を減らすことができます。

修正済みソフトウェア

修正済みソフトウェア リリースの詳細については、本アドバイザリ上部の Cisco Bug ID を参照ください。

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。

次のテーブルは該当製品および関連する Cisco バグ ID をリストします:

該当製品	この残る脆弱性は Cisco Bug ID
Nexus 3000 シリーズ スイッチ	CSCve97102
Nexus 3500 プラットフォーム スイッチ	CSCvf12757、CSCvf12804
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	CSCvf12815、CSCvf15198
Nexus 7000 シリーズ スイッチ Nexus 7700 シリーズ スイッチ マルチレイヤ ディレクタ スイッチ	CSCvb86832、CSCvd86474、CSCvd86484、CSCvd86479、CSCvd86490
Cisco Nexus 9000 シリーズ スイッチ（スタンドアロン、NX-OS モード）	CSCve97102
Cisco 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	CSCve97102

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

Cisco はこの脆弱性を発見することおよび報告するためにネットワークエンジニアに感謝することを Cody Winkler 望みます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171018-ppe

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース	—	Final	2017 年 10 月 18 日

利用規約