

# Cisco NX-OS システム ソフトウェア 対話型 TCL シェル エスケープ脆弱性

Medium	アドバイザーID : cisco-sa-20171129-nxos5	<a href="#">CVE-2017-12336</a>
m	初公開日 : 2017-11-29 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : <a href="#">4.2</a>	
	回避策 : No workarounds available	
	Cisco バグ ID : <a href="#">CSCve93763</a>	
	<a href="#">CSCvg04127</a> <a href="#">CSCve93762</a>	
	<a href="#">CSCve93750</a>	

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 TCL スクリプト サブシステムの脆弱性は対話型 TCL シェルをエスケープし、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。

ユーザが指定するファイルの不十分な入力の検証による脆弱性存在は影響を受けたデバイスの対話型 TCL シェルに通じました。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 `tclsh` 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。

このアドバイザーは、次のリンクより確認できます。

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171129-nxos5>

## 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 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
- 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

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。

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
- 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

## 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-nxos5>

## 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、単独の転載や意識を施した場合、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。