# Cisco 4000 シリーズ サービス統合型ルータ 特権EXECモード ルート シェル アクセスの脆弱性のための Cisco IOS XE ソフトウェア

| | | |
|---|---|---|
| Medium | **アドバイザリーID :** cisco-sa-20180328-privesc3<br>**初公開日 :** 2018-03-28 16:00<br>**バージョン 1.0 :** Final<br>**CVSSスコア :** 6.7<br>**回避策 :** No workarounds available<br>**Cisco バグ ID :** CSCuv91356 | CVE-2018-0183 |

**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 IOS XE ソフトウェアの CLI パーサーの脆弱性は影響を受けたデバイスの根本的な Linux シェルへのアクセス権を得、デバイスの *ルート 特権*の任意のコマンドを実行する認証された、ローカル攻撃者を可能にする可能性があります。

脆弱性はデバイスの内部データ構造にアクセスを防ぐために不適当にコマンド ライン引数をサニタイズ する影響を受けたソフトウェアが原因です。 特権EXECモード（影響を受けたデバイスへの 15）特権レベル アクセスがある攻撃者は巧妙に細工された 引数が含まれている CLI コマンドの実行によってデバイスのこの脆弱性を不正利用する可能性があります。 正常なエクスプロイトは攻撃者が影響を受けたデバイスの根本的な Linux シェルへのアクセス権を得、デバイスの *ルート 特権*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-20180328-privesc3

## 該当製品

### 脆弱性のある製品

この脆弱性は Cisco IOS XE ソフトウェアの脆弱なリリースを実行している Cisco 4000 シリーズ サービス統合型ルータに影響を及ぼします。

情報に関してはどのについての Cisco IOS XE ソフトウェアがリリースするか脆弱 で、参照しますこのアドバイザリの上で Cisco バグ ID をであって下さい。

### Cisco IOS XE ソフトウェア リリースの判別

デバイス上で実行されている Cisco IOS XE ソフトウェア リリースは、管理者がデバイスにログインして、CLI で **show version コマンド**を実行し、表示されるシステム バナーを参照することにより確認できます。 デバイスが Cisco IOS XE ソフトウェアを実行している場合、システム バナーに「*Cisco IOS Software*」、「*Cisco IOS XE Software*」などのテキストが表示されます。

次に、Cisco IOS XR ソフトウェア リリース 16.2.1 が実行されていて、インストールされているイメージ名が *CAT3K_CAA-UNIVERSALK9-M* であるデバイスでのコマンドの出力例を示します。

```
ios-xe-device# show version

Cisco IOS Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version Denali
16.2.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Sun 27-Mar-16 21:47 by mcpre
.
.
.
```

Cisco IOS XE ソフトウェア リリースのための指名および番号付与規則についての情報に関しては、Cisco IOS および NX-OS ソフトウェア レファレンスガイドを参照して下さい。

## 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 はこの脆弱性が Cisco IOS XE ソフトウェアを実行しているその他のCisco製品に影響を及ぼさないことを確認しました。

また、この脆弱性が Cisco IOS ソフトウェア、Cisco IOS XR ソフトウェア、Cisco NX-OS ソフトウェアには影響を与えないことも確認しました。

## 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詳細な情報に関しては、このアドバイザリの上で

Cisco バグ ID を参照して下さい。

Cisco IOS XE ソフトウェア リリースと Cisco IOS ソフトウェア リリースのマッピングについては、Cisco IOS XE ソフトウェアのリリースに応じて「Cisco IOS XE 2 Release Notes」、「Cisco IOS XE 3S Release Notes」、または「Cisco IOS XE 3SG Release Notes」を参照してください。

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。

## 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-20180328-privesc3

## 改訂履歴

| Version | Description | Section | Status | 日付 |
|---|---|---|---|---|
| 1.0 | 初回公開リリース | | Final | 2018-March-28 |

## 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。