

Cisco IOS XE ソフトウェア 特権EXECモード ルート シェル アクセスの脆弱性

Medium	アドバイザリーID : cisco-sa-20180926-privesc	CVE-2018-15368
	初公開日 : 2018-09-26 16:00	
	バージョン 1.0 : Final	
	CVSSスコア : 6.7	
	回避策 : No workarounds available	
	Cisco バグ ID : CSCuw45594	

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根本的な Linux ファイルシステムへの修正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。 不正利用に成功すると、攻撃者は該当デバイスの基盤となる Linux シェルの権限を奪取し、デバイス上でルート権限で任意のコマンドを実行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-20180926-privesc>

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デバイスに影響を与えます。

脆弱性が存在する Cisco IOS XE ソフトウェア リリースについては、このアドバイザリの「[修正済みソフトウェア](#)」セクションを参照してください。

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 リリースの命名と番号付けの規則に関する詳細は、『[Cisco IOS and NX-OS Software Reference Guide](#)』を参照してください。

脆弱性を含んでいないことが確認された製品

このアドバイザリの[脆弱性が存在する製品の](#)セクションにリストされている製品だけ既知この脆弱性によって影響されるためである。

シスコは、この脆弱性が Cisco IOS ソフトウェア、Cisco IOS XR ソフトウェア、および Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

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

影響を受けたおよび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、Cisco IOS ソフトウェア チェッカーを参照して下さい。

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。

Cisco IOS および IOS XE ソフトウェア

Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるよう、シスコでは [Cisco IOS Software Checker](#) ツールを提供しています。このツールにより、特定のソフトウェアリリースに該当するシスコセキュリティアドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース (「First Fixed」) を特定できます。また該当する場合、すべてのアドバイザリに記載されたすべての脆弱性が修正された最初のリリース (「Combined First Fixed」) を特定できます。

このツールを使用して次のタスクを実行できます。

- ドロップダウン リストからリリース (複数可) を選択するか、分析対象となるローカル システムからファイルをアップロードして、検索を開始する
- `show version` コマンドの出力をツールで解析する
- カスタマイズした検索 (過去に公開されたすべてのシスコセキュリティアドバイザリを検索対象に含めたり、特定のアドバイザリのみ、または最新のバンドル資料から全アドバイザリを含めるなど) を作成する

リリースが、公開されたシスコセキュリティアドバイザリのいずれかに該当するかどうかを確認するには、Cisco.com の [Cisco IOS Software Checker](#) を使用するか、以下のフィールドに Cisco IOS ソフトウェアまたは Cisco IOS XE ソフトウェア リリース (たとえば、15.1(4)M2、3.13.8S など) を入力します。

デフォルトで、Cisco IOSソフトウェアチェッカーは重要なまたは高い安全性影響定格 () がある脆弱性のためのだけ結果が含まれています。中間脆弱性のための結果が含まれるために、Cisco.com の Cisco IOSソフトウェアチェッカーを使用し、**影響定格** ドロップダウン リストの **Medium** チェックボックスをチェックして下さい。

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-20180926-privesc>

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2018-September-26

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。