# Cisco IOS XE ソフトウェア ディレクトリ トラバーサルの脆弱性

| | | |
|---|---|---|
| Medium | **アドバイザリーID :** cisco-sa-20161115-iosxe<br>**初公開日 :** 2016-11-15 16:00<br>**バージョン 1.0 :** Final<br>**CVSSスコア :** 1.5<br>**回避策 :** No workarounds available<br>**Cisco バグ ID :** CSCva60013 CSCvb22622 | CVE-2016-6450 |

**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

**パッケージ**の脆弱性は Cisco IOS XE ソフトウェアのユーティリティに基礎オペレーティング システムのいくつかのファイルに書き込み アクセスを得る認証された、ローカル攻撃者を許可する可能性があります **個々に価格をつけます**。

影響を受けたインストール ユーティリティに入る脆弱性はファイルの不十分な検証が原因です。攻撃者は影響を受けたシステムににによってアップロードし、インストール ユーティリティ指令を実行することこの脆弱性を巧妙に細工されたファイル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攻撃者が書アクセス可能なファイルを無効にし、システムの統合を妥協することを可能にする可能性がある基礎オペレーティング システムのいくつかのファイルに書き込み アクセスを得ることを可能に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、攻撃者は適切なコマンドを実行する十分な特権がなければなりません。 デフォルト 設定ではこの脆弱性を不正利用するために、 *特権 15* 特権は必要です。この脆弱性のセカンダリ影響として、攻撃者はいくつかのファイルを修正し、有効なライセンスを提供しないで基礎オペレーティング システム シェルへのアクセスを得られますかもしれません。

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。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161115-iosxe

## 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する場合以下の製品に影響を及ぼします:

- Cisco 5700 シリーズ ワイヤレス LAN コントローラ
- Cisco Catalyst 3650 シリーズ スイッチ
- Cisco Catalyst 3850 シリーズ スイッチ
- Cisco Catalyst 4500E シリーズ スイッチ
- Cisco Catalyst 4500X シリーズ スイッチ

この脆弱性はコンフィギュレーション別ではないです。 すべての先行する製品は Cisco IOS XE ソフトウェアの脆弱なリリースを実行する場合脆弱です。 脆弱なソフトウェア 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。

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特権アクセスをアクセスでき、また巧妙に細工されたファイル有能な転送ですおよびシステムの特権 コマンドを実行する必要があります。

### Cisco IOS XE ソフトウェア リリースの判別

、管理者はデバイスにログインどの Cisco IOS XE ソフトウェア リリースがデバイスで動作しているか判別し、 **show version コマンドを** Command Line Interface （ CLI ）で使用し、次に現われるシステムバナーを参照するためにできます。 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 XE Software*」などのテキストが表示されます。

次の例は Cisco IOS XE ソフトウェア リリース 3.6.5E を実行しているデバイスの **show version コマンド**の出力を示したものです:

```
Router> show version

Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M),
Version 03.06.05.E RELEASE SOFTWARE7 (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Thu 02-Jun-16 09:03 by prod_rel_team
.
.
.
```

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ついては、以下を参照してください。 ホワイト ペーパー： Cisco IOS および NX-OS ソフトウェア リファレンス ガイド

# 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。

## 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、この状況報告の上で 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

この脆弱性はデジタル セキュリティ株式会社の Maksim Malyutin によって Cisco に報告されました。

## URL

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161115-iosxe

## 改訂履歴

| Version | Description | Section | Status | 日付 |
|---|---|---|---|---|
| 1.0 | 初回公開リリース | | Final | 2016-November-15 |

## 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。