

Cisco IOS XE ソフトウェアの Web UI における特権昇格の脆弱性

Critical アドバイザリーID : cisco-sa-20170927-privesc [CVE-2017-12230](#)
初公開日 : 2017-09-27 16:00
バージョン 1.0 : Final
CVSSスコア : [9.9](#)
回避策 : No workarounds available
Cisco バグ ID : [CSCuy83062](#)

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 Web ベースのユーザ インターフェイス (Web UI) には脆弱性があり、認証されていないリモートの攻撃者により、該当するデバイス上で権限の昇格が行われる可能性があります。

この脆弱性は、該当するソフトウェアの Web UI を使用して作成される新規ユーザのデフォルトのパーミッション設定が不適切なことに起因しています。攻撃者が、該当するソフトウェアの Web UI を使用して新規ユーザを作成し、新規ユーザとして Web UI にログインすることで、この脆弱性を不正利用できる可能性があります。不正利用に成功すると、攻撃者は該当のデバイス上で権限の昇格を行う可能性があります。

この脆弱性に対処するソフトウェア アップデートは、すでにシスコからリリースされています。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-20170927-privesc>

このアドバイザリーは、2017 年 9 月 27 日に公開された 13 件の脆弱性に関する 12 件のシスコ セキュリティ アドバイザリーを含む Cisco IOS ソフトウェアおよび IOS XE ソフトウェア リリースのセキュリティ アドバイザリー バンドルの一部です。これらのアドバイザリーとリンクの一覧については、以下を参照してください。[シスコのイベント対応：9月 2017 年半年ごと Cisco IOS および IOS XE ソフトウェア Security Advisory によって組み込まれる書。](#)

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シスコ デバイスで、HTTP サーバ機能が有効な場合に影響を及ぼします。

新しく再設計された Web ベース管理 UI が、Cisco IOS XE ソフトウェアの Denali 16.2 リリースで導入されました。この脆弱性は、Cisco IOS XE ソフトウェアの以前のリリースの Web ベース管理 UI には影響を及ぼしません。

Cisco IOS XE ソフトウェアがリリースする詳細については脆弱で、見ますこの状況報告の[修正済みソフトウェアのセクション](#)をであって下さい。

Web UI 設定の確認

、管理者はデバイスにログイン Web UI がデバイスのためにイネーブルになり、設定されてかどうか判別し、**show running-config** を使用するためにできます | **http** を含んで下さい|次のコマンドの存在があるように確認する CLI の **transport** コマンド:

```
transport-map type persistent webui transport-map-name
ip http server or ip http secure-server global configuration
transport type persistent webui input transport-map-name
```

これらのコマンドが存在し、構成されている場合、Web UI が有効になっており、デバイス用に設定されています。

以下に、**show running-config | http** を含んで下さい|イネーブルになり、Web UI を使用するために設定されるルータのための **transport** コマンド:

```
Router# show running-config | include http|transport
```

```
transport-map type persistent webui https-webui
transport-map type persistent webui http-webui
no ip http server
ip http authentication local
ip http secure-server
transport type persistent webui input http-webui
```

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する場合、システム バナーは *Cisco IOS* ソフトウェア、*Cisco IOS XE* ソフトウェア、または同じようなテキストを表示します。

次の例は Cisco IOS XE ソフトウェア リリース 16.2.1 を実行して、CAT3K_CAA-

UNIVERSALK9-M のインストール済みイメージ名前があるデバイスのためのコマンドの出力を示したものです:

```
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。

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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェア アップデートを提供しています。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロードする、または、アクセスしたり、その他の方法で使用する場合、お客様は以下のリンクに記載されたシスコのソフトウェア ライセンスの条項に従うことに同意したことになります。

<https://www.cisco.com/c/en/us/products/end-user-license-agreement.html>

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限りです。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

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。

- ドロップダウンメニューからリリース (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

リリースがあらゆる公開された Cisco Security Advisory から影響を受けるとどう判別するために、Cisco.com の [Cisco IOSソフトウェアチェッカー](#) を使用するか、または一次のフィールドで... Cisco IOSソフトウェアまたは Cisco IOS XE ソフトウェア リリースを—たとえば、15.1(4)M2 か 3.13.8S 入力して下さい:

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。

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、内部セキュリティテストチームによってシスコに報告されました。

URL

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-privesc>

改訂履歴

Version	Description	Section	Status	日付
1.0	初回公開リリース		Final	2017年9月27日

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。