

Cisco IOS XE ワイヤレス コントローラ マネージャ サービス拒否の脆弱性

High

アドバイザリーID : cisco-sa-20170927-ios-xe

初公開日 : 2017-09-27 16:00

バージョン 1.0 : Final

CVSSスコア : [7.4](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvd45069](#)

[CVE-2017-12222](#)

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 ソフトウェアのワイヤレス コントローラ マネージャの脆弱性により非認証、隣接した攻撃者がスイッチの再始動を引き起こし、サービス拒否 (DoS) 状態という結果に終ることを可能にする可能性があります。

脆弱性は不十分な入力の検証が原因です。攻撃者は巧妙に細工された Association 要求を入れることによってこの脆弱性を不正利用する可能性があります。エクスプロイトは攻撃者がスイッチの再起動するために原因にな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-ios-xe>

該当製品

脆弱性のある製品

この脆弱性は IOS XE ソフトウェア バージョン 16.1 ~ 16.3.3 が稼働している、およびワイヤレス LAN コントローラ (WLC) として機能する Cisco Catalyst 3650 および 3850 スイッチに影響を与えます。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、見ますこのアドバイザリーの [修正済みソフトウェアのセクション](#)をであって下さい

。

、管理者はデバイスにログイン時の 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 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する場合、システムバナーは *Cisco IOS XE* ソフトウェアが同じようなテキストを表示する。

次の例は Cisco IOS XE ソフトウェア リリース 3.16.1aS 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 XE Software, Version 03.16.01a.S - Extended Support Release  
Cisco IOS Software, ASR1000 Software (PPC_LINUX_IOSD-ADVENTERPRISEK9-M), Version 15.5(3)S1a,  
RELEASE SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2015 by Cisco Systems, Inc.  
Compiled Wed 04-Nov-15 17:40 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、[白書を参照して下さい](#): [Cisco IOS および NX-OS ソフトウェア レファレンスガイド](#)。

、管理者はデバイスにログイン デバイスが WLC として機能したかどうか確認するために **提示ワイヤレス インターフェイス summary** コマンドを CLI で使用するためにでき、次に現われるコマンド 出力を参照します。デバイスが WLC として機能する場合、出力は設定済みインターフェイスを表示するものです。

次の例は 1 つのワイヤレス インターフェイスが設定されているデバイスの **提示ワイヤレス インターフェイス summary** コマンドの出力を示したものです：

```
3850-4# show wireless interface summary
```

```
Wireless Interface Summary
```

```
Interface Name Interface Type VLAN ID IP Address IP Netmask MAC Address
```

```
-----  
Vlan151 Management 151 192.168.151.14 255.255.255.0 d0c7.8956.b24d
```

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 ソフトウェア、Cisco IOS XR ソフトウェア、または Cisco NX-OS ソフトウェアに影響を与えないことを確認しました。

侵害のインジケータ

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。

http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.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は新規リリースでも継続して適切なサポートが受けられることを確認してください。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。

http://www.cisco.com/en/US/support/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。

修正済みリリース

顧客は Cisco IOS XE ソフトウェアにバージョン 16.3.5 をアップグレードする必要があります。

ソフトウェア アップデートは Cisco.com の [Software Center](#) からダウンロードすることができます。

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

この脆弱性はサポート ケースの解決中に発見されました。

URL

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

改訂履歴

Version	Description	Section	Status	日付
1.0	Initial public release.		Final	2017-September-27

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。