Cisco IOS XE ワイヤレス コント ローラ マネージャにおける Denial of Service（DoS）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、認証されていない隣接する攻撃者がスイッチの再起動を引き起こし、その結果サービス妨害（DoS）状態が発生する可能性があります。

この脆弱性は、入力に対する不十分な検証に起因します。 攻撃者は、巧妙に細工された関連付け要求を送信することにより、この脆弱性を不正利用する可能性があります。 この不正利用によってスイッチが再起動され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 を実行し、ワイヤレス LAN コントローラ（WLC）として機能している Cisco Catalyst 3650 および 3850 スイッチに影響を及ぼします。 Cisco IOS XE ソフトウェアがリリースする情報に関しては脆弱で、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。

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 XE Software*」などのテキストが表示されます。

次に、Cisco IOS XE ソフトウェア リリース 3.16.1aS が実行されているデバイスでの **show version** コマンドの出力例を示します。

```
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]

、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 として機能している場合、設定されたインターフェイスが出力に表示されます。

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。

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。
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ます。 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

Cisco IOS XE ソフトウェア バージョン 16.3.5 に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	初回公開リリース		Final	2017 年 9 月 27 日

利用規約