Cisco のための Cisco IOS XE ソフトウェア 5760 WLC、Cisco Catalyst 4500E Supervisor Engine 8-E および Cisco NGWC 3850 GUI 特権拡大脆弱性

High

アドバイザリーID : cisco-sa-20170927-ngwc

初公開日 : 2017-09-27 16:00

バージョン 1.0 : Final

CVSSスコア : 8.8

回避策 : No workarounds available

Cisco バグ ID : CSCvd73746

CVE-2017-12226

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 5760 ワイヤレス LAN コントローラ、Cisco Catalyst 4500E Supervisor Engine 8-E （ワイヤレス）スイッチおよび Cisco 新世代ワイヤレス コントローラ（NGWC）用の Cisco IOS XE ソフトウェアの Webベース ワイヤレス コントローラ GUI の脆弱性は 3850 影響を受けたデバイスの特権を上げる認証される、リモート攻撃者可能にする可能性があります。

脆弱性は影響を受けた GUI によって HTTP 要求の不完全な入力 検証が原因、GUI 接続状態かプロトコル変更です。 攻撃者は影響を受けたデバイスの *ロビー管理者ユーザ*としてワイヤレス コントローラ GUI に認証しか、続いて状態を変更することによってこの脆弱性または GUI への接続のためのプロトコ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特権レベルを *管理者*に上げ、影響を受けたデバイスの完全 な 制御を得ることを可能にする可能性があります。

シスコでは、本脆弱性に対処するソフトウェア アップデートをリリースしていません。 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。
927-ngwc

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 リリース 3.7.0E、3.7.1E、3.7.2E、3.7.3E、3.7.4E、または 3.7.5E を実行する場合以下のシスコ製品に影響を及ぼします:

- Cisco 5760 ワイヤレス LAN コントローラ
- Cisco Catalyst 4500E Supervisor Engine 8-E（ワイヤレス）スイッチ
- Cisco 新世代ワイヤレス コントローラ（NGWC）3850

、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** 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。

次の例は Cisco IOS XE ソフトウェア リリース 3.7.5E を実行している Cisco 5760 シリーズ ワイヤレス LAN コントローラ用の **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, 5700 Series Wireless LAN Controller Software (CT5760-
IPSERVICESK9-M), Version 03.07.5E
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
.
.
.
```

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。

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 XE ソフトウェア 3.6E リリース トレインに影響を与えないことを確認しました。 Cisco はまたこの脆弱性が 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。

さらに、Cisco はこの脆弱性が Cisco Catalyst 3650 シリーズ スイッチ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ー

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ソフトウェア アップデートを提供していません。

顧客は彼らに有効なライセンスがある機能セットおよびソフトウェア バージョンのためのサポートしかインストールし、期待しないことができます。 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/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/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

顧客はこの脆弱性を当たるための最もよいオプションを判別するために Cisco TAC に連絡する必要があります。

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 Cisco TACサポート例の解決の間に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170927-ngwc

改訂履歴

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

利用規約