Cisco IOS XE NGWC レガシー ワイヤレス デバイス マネージャGUI クロスサイト要求偽作脆弱性

Medium	**アドバイザリーID :** cisco-sa-20190821-iosxe-ngwc-csrf **初公開日 :** 2019-08-21 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 :** CSCvq64435	CVE-2019-12624

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 新世代ワイヤレス コントローラ（NGWC）のウェブベースの管理インターフェイスの脆弱性は非認証、リモート攻撃者がクロスサイト要求偽作（CSRF）攻撃を行ない、影響を受けたデバイスの任意操作を行うことを可能にする可能性があります。

脆弱性は影響を受けたソフトウェアのウェブベースの管理インターフェイスのための不十分な CSRF 保護が原因です。 攻撃者はインターフェイスのユーザを巧妙に細工されたリンクに従うように誘導す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。 正常なエクスプロイトは攻撃者が Webブラウザの使用によっておよびユーザの特権と影響を受けたデバイスの任意操作を行うことを可能にする可能性があります。

シスコはこの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ました。 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-20190821-iosxe-ngwc-csrf

該当製品

脆弱性のある製品

パブリケーションの時に、この脆弱性はの Cisco IOS XE ソフトウェアの 3.xE リリース実行した場合以下のシスコ製品に影響を及ぼしました:

- 5760 ワイヤレス LAN コントローラ
- Catalyst 3650 スイッチ
- Catalyst 3850 スイッチ
- Catalyst 4500E Supervisor Engine 8-E （ワイヤレス）スイッチ

最も完全な、現在の情報についてはこのアドバイザリの上でバグID の詳細 セクションを参照して下さい。

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性が存在する製品のセクションにリストされている製品だけ既知この脆弱性によって影響されるためにである。

Cisco はの Cisco IOS XE ソフトウェアの 16.x リリース実行する場合この脆弱性が Cisco Catalyst 3650 および 3850 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。

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

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。

修正済みリリース

Cisco IOS XE ソフトウェア

顧客が Cisco IOS XE ソフトウェアの脆弱性への公開を判別するのを助けるために Cisco はツールを、特定の Cisco IOS XE ソフトウェア リリースおよび以前のリリースに影響を与える Cisco Security Advisory を識別する Cisco IOSソフトウェア チェッカー提供します、各アドバイザリに説明がある脆弱性を解決する（「最初に」固定される）。 また該当する場合、そのリリースに関するすべてのアドバイザリ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入れたり、特定のアドバイザリのみ、または最新のバンドル資料のすべての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 から影響を受けするかどうか判別するために、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—次のフィールドで… Cisco IOS XE ソフトウェア リリースを—たとえば、**3.17.0S** 入力して下さい:

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

Cisco はこの脆弱性を報告するためにメフメット Onder キーに感謝することを望みます。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-iosxe-ngwc-csrf

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース		最終版	2019-August-21

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。