

Cisco IOSおよびIOS XEソフトウェアのWeb UIにおけるクロスサイトリクエストフォージェリの脆弱性



アドバイザーID : cisco-sa-ios-webui-

HfwnRgk

初公開日 : 2024-09-25 16:00

バージョン 1.0 : Final

CVSSスコア : [6.5](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwi59624](#) [CSCwi59625](#)

[CVE-2024-](#)

[20414](#)

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ソフトウェアおよびCisco IOS XEソフトウェアのWeb UI機能の脆弱性により、認証されていないリモートの攻撃者がWeb UIを介して該当システムにクロスサイトリクエストフォージェリ(CSRF)攻撃を実行する可能性があります。

この脆弱性は、HTTP GETメソッドを介して設定の変更を誤って受け入れることに起因します。攻撃者は、現在認証されている管理者が巧妙に細工されたリンクにアクセスするように仕向けることで、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者は該当デバイスの設定を変更でき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。

このアドバイザーは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-webui-HfwnRgk>

このアドバイザーは、Cisco IOSソフトウェアおよびIOS XEソフトウェアのセキュリティアドバイザーバンドル公開の2024年9月リリースの一部です。アドバイザーとリンクの一覧については、『[Cisco Event Response: September 2024 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication](#)』を参照してください。

該当製品

脆弱性のある製品

公開時点では、この脆弱性は、Cisco IOSソフトウェアまたはIOS XEソフトウェアの脆弱性が存在するリリースを実行していて、HTTPサーバ機能が有効になっているシスコデバイスに影響を与えました。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

HTTP サーバ設定の確認

あるデバイスで HTTP サーバが有効かどうかを判断するには、デバイスにログインし、CLI で `show running-config | include ip http server|secure|active` コマンドを使用して、グローバル コンフィギュレーションに `ip http server` コマンドまたは `ip http secure-server` コマンドがあるかどうかを確認します。| `include ip http server|secure|active` コマンドを使用して、グローバル コンフィギュレーションに `ip http server` コマンドまたは `ip http secure-server` コマンドがあるかどうかを確認します。どちらかのコマンドが含まれている場合は、HTTP サーバ機能が有効です。

以下に、`show running-config | include ip http server|secure|active` コマンドの出力を示しています。

```
<#root>
```

```
Router#
```

```
show running-config | include ip http server|secure|active
```

```
ip http server  
ip http secure-server
```

注：デバイス設定に、これらのコマンドのいずれかまたは両方が含まれている場合は、Web UI 機能が有効になっています。

`ip http server` コマンドが存在し、設定に `ip http active-session-modules none` も含まれている場合、脆弱性が HTTP 経由で 익스プロイトされることはありません。

`ip http secure-server` コマンドが存在し、設定に `ip http secure-active-session-modules none` が含まれている場合、脆弱性が HTTPS 経由で 익스プロイトされることはありません。

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[脆弱性のある製品セクション](#)に記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- IOS XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

回避策

この脆弱性に対処する回避策はありません。ただし、緩和策があります。

HTTP サーバ機能を無効にすると、この脆弱性に対する攻撃ベクトルが排除されるため、対象デバイスのアップグレードが可能になるまでの適切な対応策となる可能性があります。HTTP サーバ機能を無効にするには、グローバル コンフィギュレーション モードで `no ip http server` または `no ip http secure-server` コマンドを使用します。HTTP サーバーと HTTPS サーバーの両方を使用している場合、HTTP サーバ機能を無効にするには、両方のコマンドが必要です。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

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、シスコ セキュリティ アドバイザリ 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アップグレードソリューション一式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。

Cisco IOS および IOS XE ソフトウェア

お客様が 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に、シスコは Cisco Software Checker を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース (「First Fixed」) を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載の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。

このツールを使用するには、[「Cisco Software Checker」ページの手順に従います。](#)あるいは、

次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、[セキュリティ影響評価 \(SIR\)](#) が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。
2. リリース番号 (15.9(3)M2、17.3.3 など) を入力します。
3. [チェック (Check)] をクリックします。

2		Critical,High,Medium
このアドバイザのみ		
Enter release number	Check	

不正利用事例と公式発表

Cisco Product Security Incident Response Team (PSIRT) は、本アドバイザリに記載されている脆弱性の不正利用事例やその公表を確認していません。

出典

シスコは、この脆弱性を報告していただいたRockwell Automation社のJacek Strzalkowski氏に感謝いたします。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-webui-HfwnRgk>

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2024年9月25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。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。