Cisco IOS と Cisco IOS XE ソフトウェア UI クロスサイト リクエスト フォージェリの脆弱性

High

アドバイザリーID : cisco-sa-20200108-ios-csrf
CVE-2019-16009
初公開日 : 2020-01-08 16:00
最終更新日 : 2020-04-28 17:46
バージョン 1.1 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID : CSCvq66030

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 Web UIで見つかった脆弱性により、認証されていないリモートの攻撃者が該当デバイスでクロスサイト リクエスト フォージェリ（CSRF）攻撃を実行できる可能性があります。

この脆弱性は、該当デバイス上の Web UI の CSRF 防御が不十分なことに起因します。攻撃者は、悪意のあるリンクにアクセスするようインターフェイスのユーザを誘導することで、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、攻撃者は標的となったユーザの特権レベルで任意のアクションを実行できる場合があります。ユーザが管理者特権を持っている場合、攻撃者が該当デバイスの設定を変更したり、コマンドを実行したり、該当デバイスをリロードしたりする危険性があります。

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。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200108-ios-csrf

該当製品

脆弱性のある製品

HTTP サーバ機能が有効になっている場合、この脆弱性は、Cisco IOS または Cisco IOS XE ソ

フトウェア（16.1．1以前のリリース）の脆弱性が存在するリリースを実行しているシスコ デバイスに影響を及ぼします。Cisco IOS および Cisco IOS XE ソフトウェアにおける HTTP サーバ機能のデフォルトの状態は、バージョンによって異なります。

脆弱性が存在する Cisco IOS ソフトウェアおよび Cisco IOS XE ソフトウェアのリリースについての詳細は、このアドバイザリの「修正済みソフトウェア」の項を参照してください。

HTTP サーバ設定の確認

HTTP サーバ機能がデバイスで有効かどうかを確認するには、管理者がデバイスにログインして 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。どちらかのコマンドが含まれ、設定されている場合は、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：デバイス設定にどちらかのコマンドまたは両方のコマンド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 経由でエクス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 経由でエクス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 Cisco IOS XR ソフトウェアまたは 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。

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。管理者は、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 コマンドを使用して、HTTP サーバ機能を無効にすることができます。HTTP サーバと HTTP セキュア サーバの両方が使用されている場合、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。

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リリースしています。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、アクセスまたはその他の方法で使用した場合、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/c/en/us/products/end-user-license-agreement.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、[シスコのセキュリティアドバイザリおよびアラート（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 Cisco Service Contract 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 POS 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/c/en/us/support/web/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。

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するため、シスコは Cisco IOS Software Checker ツールを提供しています。このツールを使用すると、特定のソフトウェア リリースに該当するシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。また該当する場合、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 リストからリリース（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、公開されたシスコセキュリティアドバイザリのいずれかに該当するかどうかを確認するには、Cisco.comのCisco IOS Software Checkerを使用するか、以下のフィールドにCisco IOSまたはIOS XEソフトウェアリリース(たとえば、15.1(4)M2、3.13.8Sなど)を入力します。

Check

デフォルトでは、Cisco IOS ソフトウェアのチェックには、結果は、高セキュリティへの影響の評価 (サー) または重大な脆弱性にのみが含まれています。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com の Cisco IOS ソフトウェア チェッカーを使用して、[Impact Rating] ドロップダウン リストの [中間（Medium）] チェックボックスをオンにします。

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

この脆弱性を報告していただいた Mehmet Önder Key 氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200108-ios-csrf

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.1	"show running-config | include ip http server|secure」コマンドを「show running-config | include ip http server|secure|active」と入力します。	該当製品	Final	2020 年 4 月 28 日
1.0	初回公開リリース	—	Final	2020 年 1 月 8 日

利用規約

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。