Cisco IOS XEソフトウェアのWeb UI反映クロスサイトスクリプティングの脆弱性

Medium

アドバイザリーID : cisco-sa-webui-xss-VWyDgjOU
初公開日 : 2025-09-24 16:00
バージョン 1.0 : Final
CVSSスコア : 6.1
回避策 : No workarounds available
Cisco バグ ID : CSCwm57073

CVE-2025-20240

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の脆弱性により、認証されていないリモートの攻撃者が、影響を受けるデバイスで反映されたクロスサイトスクリプティング攻撃(XSS)を実行する可能性があります。

この脆弱性は、ユーザが入力した入力の不適切なサニタイズが原因です。攻撃者は、悪意のあるリンクをクリックするようにユーザを誘導することで、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は反映されたXSS攻撃を実行し、該当デバイスからユーザのCookieを盗む可能性があります。

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-webui-xss-VWyDgjOU

このアドバイザリは、Cisco IOSおよびIOS XEソフトウェアのセキュリティアドバイザリバンドル公開の2025年9月リリースの一部です。これらのアドバイザリとリンクの一覧については、『シスコイベントレスポンス：Cisco IOSおよびIOS XEソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年9月）』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、HTTPまたはHTTPSが有効で、WebAuthが有効になっている場合、この脆弱性はCisco IOS XEソフトウェア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

デバイスで HTTP サーバー機能が有効になっているかを確認するには、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ている場合は、HTTP サーバー機能が有効です。

以下の例は、HTTP サーバー機能が有効になっているデバイスで show running-config | include ip http server|secure|active コマンドを実行した場合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ベースの管理インターフェイス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 が含まれている場合、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。

スイッチのWebAuth設定の確認

WebAuth機能がデバイスで有効になっている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 proxy httpコマンドを使用して、proxy httpコマンドが存在するかどうかを確認します。このコマンドが存在する場合、デバイスに対してWebAuth機能が有効になっています。

次に、WebAuth機能が有効になっているデバイスでのshow running-config | include proxy httpコマンドの出力例を示します。

```
<#root>

Router#

show running-config | include proxy http


ip admission

proxy http

 success redirect http://www.cisco.com
ip admission name webauth1

proxy http
```

WLCのWebAuth設定の決定

Web認証機能がデバイスで有効になっているかどうかを確認するには、デバイスにログインし、CLIでshow running-config | include parameter-mapコマンドを使用して、パラメータマップタイプwebauthが存在するかどうかを確認します。パラメータマップタイプwebauthが存在する場合、そのデバイスに対してWebAuth機能が有効です。

次に、WebAuth機能が有効になっているデバイスでのshow running-config | include parameter-mapコマンドの出力例を示します。

```
<#root>

Router#

show running-config | include parameter-map


parameter-map type

webauth

 global
parameter-map type

webauth

 webauthtest
security

web-auth

 parameter-map webauthtest
```

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リストされている製品だけがこの脆弱性の影響を受けることが知られています。

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 ソフトウェア
- IOS XR ソフトウェア
- 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。

HTTP サーバ機能を無効にすると、こうした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 サーバー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 サーバー機能を無効にするには、両方のコマンドが必要です。

信頼できるネットワークだけにHTTPサーバへのアクセスを許可すると、これらの脆弱性による影響を制限できます。次の例は、信頼できる 192.168.10.0/24 ネットワークから HTTP サーバへのリモートアクセスを許可する方法を示しています。

```
!
ip http access-class ipv4 restrict_ipv4_webui
!
ip access-list standard restrict_ipv4_webui
permit 192.168.10.0 0.0.0.255
!
```

詳細については、「アクセスリストを使用してCisco IOS XEデバイスWebUI宛てのトラフィックをフィルタリングする」を参照してください。

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

シスコでは、修正済みソフトウェアリリースへのアップグレードが利用可能になるまで、回避策や緩和策は一時的な解決策であると考えています。この脆弱性を完全に修復し、本アドバイザリ

で説明されている障害の発生を回避するために、お客様には本アドバイザリで説明されている修正済みソフトウェアにアップグレードすることを強く推奨します。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS 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（例：15.9(3)M2、17.3.3）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、アドバイザリで説明されている脆弱性に対して概念実証段階のエクスプロイト コードが入手可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

出典

シスコは、この脆弱性を報告していただいたTraboda CyberLabsのAswin M Guptha氏とAbhinand N氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-

xss-VWyDgjOU

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	2025年9月24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。