Cisco IOS XEソフトウェアのWebベース管理インターフェイスにおけるDenial of Service(DoS)の脆弱性

Medium

アドバイザリーID : cisco-sa-xe-webui-dos-PtAODAWW　CVE-2026-20311
初公開日 : 2026-08-05 16:00
バージョン 1.0 : Final
CVSSスコア : 6.3
回避策 : No workarounds available
Cisco バグ ID : CSCwu25287

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ベース管理インターフェイスにおける脆弱性により、権限の低い認証されたリモート攻撃者が、該当デバイスでサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、Webベースの管理インターフェイスでのエラー処理が不十分であることに起因します。攻撃者は、不正な証明書で認証を行うことで、この脆弱性をエクスプロイトする可能性があります。不正利用に成功すると、攻撃者は該当デバイスのリロードを引き起こし、その結果 DoS 状態が発生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-xe-webui-dos-PtAODAWW

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 XEソフトウェアの脆弱性が存在するリリースを実行し、Personal Identity Verification(PIV)を有効にしたHTTPサーバ機能を持つシスコデバイスに影響を与えました。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、バージョンとプラットフォームによって異なります。

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、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 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。

PIV設定の確認

PIVベースの認証が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て、CLIでshow running-config | include http secure-piv-based-authコマンドを使用します。出力がある場合は、次の例に示すように、PIVベースの認証が有効になっています。

```
<#root>

Router#

show running-config | include http secure-piv-based-auth
```

```
ip http secure-piv-based-auth secure-piv-based-author-only
Router#
```

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。

修正済みソフトウェア

シスコでは、回避策や緩和策（該当する場合）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の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正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載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、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James氏に感謝いたします。

URL

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

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	2026年8月5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。