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-webui-dos-qdc7qx3
初公開日 : 2026-08-05 16:00
バージョン 1.0 : Final
CVSSスコア : 4.3
回避策 : No workarounds available
Cisco バグ ID : CSCwu19075

CVE-2026-20308

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、該当デバイスに対してサービス妨害(DoS)攻撃を実行する可能性があります。

この脆弱性は、不十分な入力検証に起因します。攻撃者は、巧妙に細工された入力を該当デバイスのWebベース管理インターフェイスに送信することにより、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Webベースの管理インターフェイスを応答不能に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-dos-qdc7qx3

該当製品

脆弱性のある製品

公開時点で、Webベースの管理インターフェイスが有効になっているCisco IOS XEソフトウェアはこの脆弱性の影響を受けました。

注：Webベースの管理インターフェイスをイネーブルにするには、ip http serverまたはip http secure-serverコマンドを使用します。

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。

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。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、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 XE ソフトウェア

お客様がCisco IOS XEソフトウェアの脆弱性による侵害を受ける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

この脆弱性を報告していただいたCipher社に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-dos-qdc7qx3

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

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。

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。