

Cisco IOS XEソフトウェアのHTTP APIにおけるコマンドインジェクションの脆弱性



アドバイザリーID : cisco-sa-ios-xe-cmd-inject-rPJM8BGL

[CVE-2025-20334](#)

初公開日 : 2025-09-24 16:00

バージョン 1.0 : Final

CVSSスコア : [8.8](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwn48408](#)

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HTTP APIサブシステムにおける脆弱性により、リモート攻撃者が、root権限で実行するコマンドを基盤となるオペレーティングシステムに注入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。管理者権限を持つ攻撃者は、該当システムへの認証を行い、巧妙に細工された入力を使用してAPIコールを実行することにより、この脆弱性をエクスプロイトする可能性があります。または、認証されていない攻撃者が、システムに現在ログインしている管理者権限を持つ正当なユーザに、巧妙に細工されたリンクをクリックするように説得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rootユーザとして任意のコマンドを実行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-xe-cmd-inject-rPJM8BGL>

このアドバイザリーは、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ーバンドル公開の2025年9月リリースの一部です。これらのアドバイザリー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ー公開資料 \(半年刊、2025年9月 \)](#)』を参照してください。

該当製品

脆弱性のある製品

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及ぼします。

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 サーバ機能が有効です。

以下の例は、HTTP サーバ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
```

`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。

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、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

この脆弱性は、シスコの社内セキュリティテストで発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cmd-inject-rPJM8BGL>

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

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。