# Cisco IOSソフトウェアおよびIOS XEソフトウェアリリース3EのHTTPサーバにおけるDoS脆弱性

High

アドバイザリーID : cisco-sa-ios-http-dos-sbv8XRpL
初公開日 : 2026-03-25 16:00
バージョン 1.0 : Final
CVSSスコア : 7.7
回避策 : No workarounds available
Cisco バグ ID : CSCwq14981

CVE-2026-20125

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ソフトウェアおよびCisco IOS XEソフトウェアリリース3EのHTTPサーバ機能の脆弱性により、認証されたリモート攻撃者が該当デバイスの予期しないリロードを引き起こし、その結果、サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、ユーザー入力の検証が不適切なことに起因します。攻撃者は、不正なHTTP要求を該当デバイスに送信することで、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、攻撃者はウォッチドッグタイマーを時間切れにしてデバイスをリロードさせ、結果としてDoS状態を引き起こす可能性があります。この脆弱性を不正利用するには、攻撃者は有効なユーザアカウントを持っている必要があります。

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-ios-http-dos-sbv8XRpL

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2026年3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、『Cisco Event Response: March 2026 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication』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ソフトウェアまたはIOS XEソフトウェアリリース3Eの脆弱性が存在するリリースを実行し、アクティブなWEB_EXECモジュールで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与えます。

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

脆弱性のあるソフトウェアリリースを実行しているデバイスが、脆弱性のある設定を使用しているかどうかを確認するには、次の手順を実行します。

ステップ 1：HTTPサーバが有効になっているかどうかの確認

デバイスでHTTPサーバ機能が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 ip http server|secure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コマンドが存在す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。

次の例は、HTTPサーバ機能が有効になっているデバイスでのshow running-config | include ip http server|secure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、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。

コマンドの出力が返された場合は、ステップ2に進みます。出力が空の場合、デバイスはこの脆弱性の影響を受けません。

ステップ 2WEB_EXECモジュールがアクティブかどうかの確認

デバイスがWEB_EXECモジュールを使用しているかどうかを確認するには、CLIでshow ip http server session-module | include Status|WEB_EXECコマンドを使用します。

ステップ1の出力にip http serverが含まれている場合、コマンド出力のStatusの値を確認します。StatusがActiveの場合、デバイスはHTTPによるこの脆弱性の影響を受けます。

ステップ1の出力にip http secure-serverが含まれている場合、コマンド出力のSecure-statusの値を確認します。Secure-statusがActiveの場合、デバイスはHTTPSに関するこの脆弱性の影響を受けます。

次の例は、show ip http server session-module | include Status|WEB_EXECコマンドの出力を示しています。Web_EXECのStatusとSecure-statusはどちらもInactiveであるため、このデバイスはこの脆弱性の影響を受けません。

```
<#root>

Router#

show ip http server session-module | include Status|WEB_EXEC

 Session module Name  Handle

Status   Secure-status

     Description

WEB_EXEC

              5

Inactive Inactive

          HTTP based IOS EXEC Server
```

次の例は、両方の手順のコマンドの出力を示しています。HTTPSサーバのみが有効で、WEB_EXECのSecure-statusがInactiveであるため、このデバイスはこの脆弱性の影響を受けません。

```
<#root>

Router#

show running-config | include ip http server|secure

ip http

secure-server

Router#
```

```
show ip http server session-module | include Status|WEB_EXEC

 Session module Name  Handle
Status   Secure-status
     Description
WEB_EXEC
              5
Active   Inactive
          HTTP based IOS EXEC Server
```

### 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 XE 16およびIOS XE 17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

この脆弱性は、内部セキュリティテストで Cisco Advanced Security Initiatives Group（ASIG）の T.VE によって発見されました。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-http-dos-sbv8XRpL

## 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3月25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。