

# Cisco IOx Application Hosting Environmentの保存されたクロスサイトスクリプティングの脆弱性



アドバイザーID : cisco-sa-iox-xss-

LpGkzwtJ

初公開日 : 2026-03-25 16:00

バージョン 1.0 : Final

CVSSスコア : [4.8](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCWq69484](#)

[CVE-2026-](#)

[20112](#)

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ベースのCisco IOxアプリケーションホスティング環境管理インターフェイスにおける脆弱性により、認証されたリモートの攻撃者が、該当デバイスのWebベース管理インターフェイスのユーザに対してストアドクロスサイトスクリプティング(XSS)攻撃を実行する可能性があります。

この脆弱性は、ユーザ指定の入力の検証が不十分であることに起因します。攻撃者は、悪意のあるコードをインターフェイスの特定のページに挿入することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は該当インターフェイスのコンテキストで任意のスクリプトコードを実行したり、ブラウザベースの機密情報にアクセスする可能性があります。この脆弱性を不正利用するには、攻撃者は有効な管理者クレデンシャル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-iox-xss-LpGkzwtJ>

このアドバイザーは、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ーバンドル公開の2026年3月リリースの一部です。これらのアドバイザー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

公開時点では、Cisco IOxアプリケーションホスティング環境用に設定された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するシスコデバイスに、この脆弱性の影響が及んでいました。Cisco IOxアプリケーションホスティング環境は、デフォルトでは設定されていません。

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。

### IOx アプリケーション ホスティング構成の確認

Cisco IOS XEソフトウェアでCisco IOxアプリケーションホスティング環境が設定されているかどうかを確認するには、次の例に示すように、特権EXECモードでshow run | include ioxコマンドを使用します。

```
Switch#show run | include iox  
iox
```

上の例に示すように、出力にioxのみの行が含まれている場合、そのデバイスはこの脆弱性の影響を受けます。

### 脆弱性を含ま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、Cisco IOxアプリケーションホスティング環境をサポートする次のシスコ製品がこの脆弱性の影響を受けないことを確認しました。

- 800 シリーズ産業用サービス統合型ルータ ( ISR )
- Catalyst 3650 シリーズ スイッチ
- Catalyst 3850 シリーズ スイッチ
- Catalyst 9100 アクセスポイントファミリ ( COS-AP )
- CGR1000コンピューティングモジュール
- IC3000産業用コンピューティングゲートウェイ
- IR510 WPAN 産業用ルータ
- IOS ソフトウェア

- NX-OS ソフトウェア

また、この脆弱性がCisco IOS XRソフトウェアには影響を与えないことも確認しました。

## 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た脆弱性

の公開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OPSWATのユニット515チームに感謝いたします。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-xss-LpGkzwtJ>

## 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。