

Cisco CatalystおよびRuggedシリーズスイッチ用Cisco IOS XEソフトウェアのセキュアブートバイパスの脆弱性



アドバイザリーID : [cisco-sa-xe-secureboot-CVE-2026-bypass-B6uYxYSZ](#) [CVE-2026-20104](#)

初公開日 : 2026-03-25 16:00

バージョン 1.0 : Final

CVSSスコア : [6.1](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCws75667](#) [CSCwr77016](#)

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 Catalyst 9200シリーズスイッチ、Cisco Catalyst ESS9300エンベデッドシリーズスイッチ、Cisco Catalyst IE9310およびIE930用Cisco IOS XEソフトウェアのブートローダにおける脆弱性20 Ruggedシリーズスイッチ、Cisco IE3500およびIE3505 Ruggedシリーズスイッチでは、レベル15権限を持つ認証されていないローカルの攻撃者、または該当デバイスに物理的にアクセスする認証されていない攻撃者が、ブート時に任意のコードを実行して、信頼のチェーンを破壊する可能性があります。

この脆弱性は、ブート時のソフトウェアの検証が不十分であることに起因します。攻撃者は、該当デバイスにロードされたバイナリを操作して、ブートプロセス中に実行される整合性チェックの一部をバイパスすることにより、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、Cisco署名付きイメージを実行する要件を回避するコードを実行できる可能性があります。

シスコはこのセキュリティアドバイザリーのスコアに「中」ではなく「高」のSecurity Impact Rating(SIR)を割り当てました。これは、この脆弱性によって攻撃者がデバイスの主要なセキュリティ機能をバイパスできるようになるためです。

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-xe->

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、デバイス設定に関係なく、Cisco IOS XEソフトウェアの脆弱性のあるリリースを実行する次のシスコ製品に影響を与えます。

- Catalyst 9200シリーズスイッチ (9200CXおよび9200Lスイッチを含む)
- Catalyst ESS9300 エンベデッド シリーズ スイッチ
- Catalyst IE9310およびIE9320高耐久性シリーズスイッチ
- IE3500およびIE3505高耐久性シリーズスイッチ

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。

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
- このアドバイザリの「[脆弱性のある製品](#)」セクションに記載されているデバイス以外のデバイスで実行されているIOS XE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

ト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

本脆弱性は、シスコ内部でのセキュリティ テストによって発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xe-secureboot-bypass-B6uYxYSZ>

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

本アドバイザー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。本アドバイザー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。

本アドバイザー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。