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

High

アドバイザリーID : cisco-sa-secboot-UqFD8AvC
初公開日 : 2025-09-24 16:00
バージョン 1.0 : Final
CVSSスコア : 6.7
回避策 : No workarounds available
Cisco バグ ID : CSCwo38903 CSCwo38924

CVE-2025-20313
CVE-2025-20314

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ソフトウェアの複数の脆弱性により、レベル15権限を持つ認証されたローカル攻撃者、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、ブート時に永続的な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。

これらの脆弱性は、ソフトウェアパッケージの不適切な検証に起因します。攻撃者は、該当デバイスの特定の場所に巧妙に細工されたファイルを配置することにより、これら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、基盤となるオペレーティングシステムで永続的なコードが実行される可能性があります。

これらの脆弱性により、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、シスコはこのアドバイザリのセキュリティ影響評価(SIR)を中から高に引き上げました。

シスコはこれら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。これら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-secboot-UqFD8AvC

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2025年9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、『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

これらの脆弱性は、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する次のシスコ製品に影響を与えます。

次の表に、影響を受けるハードウェアプラットフォームと、影響を受ける最初のソフトウェアリリースを示します。

シスコ プラットフォーム	影響を受ける最初のリリース
1000 シリーズ サービス統合型ルータ	17.8.1
1100 ターミナル サービス ゲートウェイ	17.7.1
4000 シリーズ サービス統合型ルータ	17.3.1
8100シリーズセキュアルータ	17.15.1
8400シリーズセキュアルータ	17.12.1
ASR 1000 シリーズ アグリゲーション サービス ルータ	17.7.1
C8375-E-G2プラットフォーム	17.15.3
Catalyst IE 3300高耐久性シリーズルータ	17.12.1
Catalyst IR1100高耐久性シリーズルータ	17.13.1
Catalyst IR8100ヘビーデューティシリーズルータ	17.4.1
Catalyst IR8300 高耐久性シリーズ ルータ	17.7.1
Catalyst 8200 シリーズ エッジ プラットフォーム	17.8.1
Catalyst 8300 シリーズ エッジ プラットフォーム	17.8.1
Catalyst 8500L エッジプラットフォーム	17.8.1
Catalyst 9200 シリーズ スイッチ	17.8.1
エンベデッドサービス3300シリーズ	17.12.1
VG410アナログ音声ゲートウェイ	17.17.1

脆弱性のある Cisco ソフトウェアリリースの詳細については、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」セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

シスコは、これらの脆弱性が次のシスコ製品に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

これら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。これらの脆弱性を完全に修正し、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）では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

出典

CVE-2025-20313：この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のAndrew Kimによる内部セキュリティテストで発見されました。

CVE-2025-20314：この脆弱性は、Cisco ASIGのArthur Vidineyevによる内部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-secboot-UqFD8AvC

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

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。