

Cisco IOS XRソフトウェアイメージ検証バイパスの脆弱性



アドバイザリーID : cisco-sa-ios-xr-verii-

bypass-HhPwQRvx

初公開日 : 2025-03-12 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 : [CSCwk67262](#)

[CVE-2025-](#)

[20177](#)

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 XRソフトウェアのブートプロセスにおける脆弱性により、認証されたローカル攻撃者がCisco IOS XRイメージの署名の検証をバイパスし、未検証のソフトウェアを該当デバイスにロードする可能性があります。この脆弱性を不正利用するには、攻撃者は該当デバイスでroot-system権限を持っている必要があります。

この脆弱性は、ブート検証プロセスにおけるファイルの検証が不完全であることに起因します。攻撃者は、システム設定オプション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、攻撃者はブート設定を制御できるようになり、シスコ署名イメージを実行する要件を回避したり、実行中のシステムのセキュリティプロパティを変更したりすることが可能になります。

注：この脆弱性のエクスプロイトにより、攻撃者がシスコのイメージ検証をバイパスする可能性があるため、シスコはこのアドバイザリー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-xr-verii-bypass-HhPwQRvx>

このアドバイザリーは、Cisco IOS XRソフトウェアSecurity Advisoryバンドル公開の2025年3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](#)

[ス: Cisco IOS XRソフトウェアセキュリティアドバイザリバンドル公開の半年刊2025年3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、デバイス設定に関係なく、Cisco IOS XR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。

- 8000 シリーズ ルータ
- NCS540Lイメージを実行しているNetwork Convergence System(NCS)540シリーズルータ
- NCS 1010
- NCS 1014
- NCS5700イメージを実行しているNCS 5700シリーズ固定ポートルータ

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、Cisco IOS XRソフトウェアを実行している次のシスコ製品には、この脆弱性が影響を与えないことを確認しました。

- ASR 9000 シリーズ ルータ
- IOS XRd vRouter
- IOS XRV 9000 ルータ
- NCS 540シリーズルータNCS540-ACC-SYSおよびNCS 540-24Z8Q2C-SYS
- NCS 5500 シリーズ ルータ
- NCS 5700シリーズ固定ポートルータNCS-57C3-MOD-SおよびNCS-57C3-MOD-SE-S

また、シスコは、これら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 XE 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

シスコはこのアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースしています。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェア アップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

<https://www.cisco.com/c/en/us/products/end-user-license-agreement.html>

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限りです。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の [シスコサポート & ダウンロードページ](#)には、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス (My Devices)] ツールを使用するお客様のカスタマーデバイスサポート範囲も表示できます。

[ソフトウェアのアップグレード](#)を検討する際には、[シスコ セキュリティ アドバイザリ ページ](#)で入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレード ソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center (TAC) もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC (https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html) に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次の表では、左の列にシスコ ソフトウェア リリースまたはトレインを記載しています。右側の列は、リリース (トレイン) がこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。

Cisco IOS XR ソフトウェア リリース	First Fixed Release (修正された最初のリリース)
7.10 以前	修正済みリリースに移行。
7.11	7.11.21
24.2	24.2.2
24.3	24.3.2
24.4	24.4.1

注：シスコでは、この脆弱性に対処するSMUをリリースしません。

Product Security Incident Response Team (PSIRT; プロダクト セキュリティ インシデント レスポンス チーム) は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

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-ios-xr-verii-bypass-HhPwQRvx>

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3月12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。

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。