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-xrsig-UY4zRUCG
初公開日 : 2025-09-10 16:00
バージョン 1.0 : Final
CVSSスコア : 6.0
回避策 : No workarounds available
Cisco バグ ID : CSCwm03455

CVE-2025-20248

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ソフトウェアのインストール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ソフトウェアのイメージ署名の検証をバイパスし、未署名のソフトウェアを該当デバイスにロードできる可能性があります。この脆弱性をエクスプロイトするには、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、.isoファイルのインストール中の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、.isoイメージの内容を変更してからデバイスにインストールしてアクティブ化することで、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、攻撃者はイメージアクティベーションプロセスの一部として署名されていないファイルをロードできる可能性があります。

注：この脆弱性がエクスプロイトされると、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のセキュリティ影響評価（SIR）を [中（Medium）] から [高（High）] 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-xrsig-UY4zRUCG

このアドバイザリは、Cisco IOS XRソフトウェアSecurity Advisory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 XR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

この脆弱性は、デバイスの設定に関係なく、Cisco IOS XR ソフトウェアの脆弱性が存在するリリースを実行している以下のシスコ製品に影響を与えます。

- ASR 9000 シリーズ アグリゲーション サービス ルータ（64 ビット）
- IOS XR ホワイトボックス（IOSXRWBD）
- IOS XRv 9000 ルータ
- NCS 540-iosxrベースイメージを実行しているNetwork Convergence System(NCS)540シリーズルータ
- NCS 560 シリーズ ルータ
- NCS 1000シリーズ（NCS 1001、NCS 1002、およびNCS 1004）
- NCS 5000 シリーズ ルータ
- NCS 5500 シリーズ ルータ
- NCS 5500ベースイメージを実行しているNCS 5700シリーズラインカードおよびルータ
- NCS 6000 シリーズ 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
- IOS XE ソフトウェア
- NX-OS ソフトウェア

また、次のシスコデバイスで実行されているCisco IOS XRソフトウェアも、この脆弱性の影響を受けません。

- 8000 シリーズ ルータ
- NCS 540L-iosxrベースイメージを実行しているNCS 540シリーズルータ
- NCS 1010プラットフォーム
- NCS 1014プラットフォーム
- NCS 5700ベースイメージを実行しているNCS 5700シリーズデバイス

詳細

この脆弱性をエクスプロイトするには、該当デバイスでroot-system権限を持つ攻撃者が、修正された.isoイメージをインストールして、ソースをアクティブ化する必要があります。この脆弱性の修正により、.isoイメージ内のファイルに対する追加チェックが導入され、署名されていないファイルがインストールされないようになります。

お客様は、修正済みリリースからの予期しないダウングレードについてデバイスを監視する必要があります。これは、この修正が古いバージョンには適用されないためです。

インストール先のデバイス上のイメージに対して計算されたMD5またはSHA512チェックサムと、Cisco.comにリストされているそのイメージの対応するMD5またはSHA512チェックサムを比較して、ソフトウェアイメージの整合性を検証することをお勧めします。

ソフトウェアイメージの整合性を検証するために実行する必要がある手順を示す次の例では、純正のCisco IOS XRソフトウェアリリース7.10.2 .isoファイルと無効なファイルが比較されています。

1. Cisco Software Downloadページで、Cisco IOS XRソフトウェアリリース7.10.2の.isoファイルのMD5およびSHA512チェックサム値をチェックします。これらの値は次のとおりです。

- MD5チェックサム：1c79e3ece14e4cd873f02cd70693af85
- SHA512チェックサム：

```
0d6c6f4469f0034072b819f7e576639f46dfd033b3920574c767fc39fa14ea850928c8ecf
```

2. 次の例に示すように、ハードディスクからインストールされるチェックサムを、Cisco.comから予期されるチェックサムと共に検証します。

ハードディスクからインストールされるasr9k-mini-x64-7.10.2.isoのSHA512チェックサムが、Cisco.comから予測されるチェックサムと一致します。

```
<#root>

RP/0/RSP0/CPU0:Router#

run sha512sum /harddisk:/asr9k-mini-x64-7.10.2.iso


Wed Sep 10 16:00:00.000 UTC
0d6c6f4469f0034072b819f7e576639f46dfd033b3920574c767fc39fa14ea850928c8ecf2ae4bb233b57e46cd5580b14fa5bdb
RP/0/RSP0/CPU0:Router#
```

asr9k-mini-x64-7.10.2.iso のMD5チェックサムが、Cisco.comから予想されるチェックサムと一致しません。

```
<#root>

RP/0/RSP0/CPU0:Router#

show md5 file /harddisk:/asr9k-mini-x64-7.10.2.iso


Wed Sep 10 16:00:00.000 UTC

4acce5bb525cc47da0adb5fcb330e0f5

  /harddisk:/asr9k-mini-x64-7.10.2.iso
RP/0/RSP0/CPU0:Router#
```

チェックサムが一致しない場合は、イメージをインストールしないでください。

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ます。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	修正済みリリースに移行。
24.2	24.2.21
24.3	修正済みリリースに移行。
24.4	24.4.2
25.1	影響なし。

この脆弱性に対して作成されたSMUはありません。SMUは実行可能ですが、変更された.isoイメージをインストールしてアクティブ化できる攻撃者はすべて、不正利用される前にSMUを削除できる可能性もあります。

シスコの 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済み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

この脆弱性を報告してくださった外部の研究者に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xrsig-UY4zRUCG

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10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。