Cisco IOS XR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-xr-secure-boot-quD5g8Ap
CVE-2024-20456
初公開日 : 2024-07-10 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 : CSCwk58609

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、高い権限を持つ認証されたローカルの攻撃者がCisco Secure Boot機能をバイパスし、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、ソフトウェア構築プロセスのエラーに起因します。攻撃者は、システムの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、攻撃者はブート設定を制御し、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できるようになります。

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-xr-secure-boot-quD5g8Ap

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOS XRリリース24.2.1を実行している次のシスコ製品に影響を与えます。

- 8000 シリーズ ルータ
- NCS 1010 シリーズ ルータ
- NCS 1014 シリーズ ルータ
- NCS540L イメージを実行している NCS 540 シリーズ ルータ
- NCS 5700固定ポートシリーズルータ（NCS-57C3-MOD-SおよびNCS-57C3-MOD-SE-Sを除く）

注：Cisco IOS XRリリース24.2.1のみが脆弱なリリースです。

ソフトウェアリリースを確認する

デバイスが該当のソフトウェアイメージを実行しているかどうかを確認するには、デバイスの CLI で show version コマンドを実行します。次の例に示すように、上記の該当製品でバージョン24.2.1が実行されていることが出力に示されている場合、そのデバイスはこの脆弱性の影響を受けています。

```
<#root>

Router#

show version

Cisco IOS XR Software, Version

24.2.1

Copyright (c) 2013-2024 by Cisco Systems, Inc.
```

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、この脆弱性が次のCisco IOS XR製品には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 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固定ポートシリーズルータNCS-57C3-MOD-SおよびNCS-57C3-MOD-SE-S

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

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アップグレード ソリューション一式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

この問題は、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プラットフォームで実行されているCisco IOS XRリリース24.2.1のみに影響します。修正リリースは24.2.11です。

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-xr-secure-boot-quD5g8Ap

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	2024年7月10日

利用規約

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。