Cisco IOS XRソフトウェアのiPXEブートシグニチャバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-iosxr-ipxe-sigbypass-pymfyqgB
CVE-2023-20236
初公開日 : 2023-09-13 16:00
最終更新日 : 2024-03-14 17:35
バージョン 2.1 : Final
CVSSスコア : 6.7
回避策 : No workarounds available
Cisco バグ ID : CSCwh78727 CSCwh78724 CSCwi26526 CSCwe12502 CSCwh70601 CSCvz63918 CSCvz63929 CSCwi31568 CSCvz63925

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iPXEブート機能における脆弱性により、認証されたローカルの攻撃者が、該当デバイスに未検証のソフトウェアイメージをインストールする可能性があります。

この脆弱性は、イメージの検証が不十分であることに起因します。攻撃者は、該当デバイスのiPXEブートプロセス中にイメージ検証のブートパラメータを操作することで、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、攻撃者は該当デバイス上の未検証のソフトウェアイメージをブートできる可能性があります。

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-iosxr-ipxe-sigbypass-pymfyqgB

このアドバイザリは、2023年9月に公開された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の一部です。アドバイザリの全リストとそのリンクについては、『Cisco Event Response: Seemannual Cisco IOS XR 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

公開時点では、この脆弱性は、Cisco IOS XRソフトウェアの脆弱性のあるリリースを実行している次のシスコ製品に影響を与えました。

- 8000 シリーズ ルータ
- ASR 9000 シリーズ アグリゲーション サービス ルータ
- 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 4000 シリーズ
- NCS 5000 シリーズ
- NCS 5500 シリーズ
- NCS 5700 シリーズ

公開時点で脆弱性が確認されている Cisco ソフトウェアの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。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細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

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。

修正済みリリース

公開時点では、次の表に示すリリース情報は正確でした。最も完全で最新の情報については、このアドバイザリの上部にあるバグ ID の詳細セクションを参照してください。

次の表では、左の列にこのアドバイザリに記載された脆弱性の影響を受けるシスコデバイスを、右の列にこの脆弱性に対する修正を含むリリースを示します。

シスコ プラットフォーム	First Fixed Release（修正された最初のリリース）
8000 シリーズ ルータ	7.10.1
ASR 9000シリーズLightspeedベースのラインカード	24.1.1
ASR 9000シリーズTomahawkベースのラインカード	計画なし
NCS 560	24.2.1
NCS 1001	計画なし
NCS 1002	計画なし
NCS 1004	24.1.1
NCS 4000	計画なし
NCS 5500	7.10.1
NCS 5700	7.10.1

シスコはこれらの脆弱性に対処するSMUをリリースしていません。

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-iosxr-ipxe-sigbypass-pymfyqgB

改訂履歴

バージョン	説明	セクション	ステータス	日付
2.1	「修正済みリリース」セクションを更新。	修正済みリリース	Final	2024年3月14日
2.0	この脆弱性の影響を受けるデバイスに関する情報を含む修正済みリリースの表を追加。	修正済みリリース	Final	2024年3月13日
1.0	初回公開リリース	—	Final	2023年9月13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。