Cisco IOS XRソフトウェアイメージ検証の脆弱性

Medium

アドバイザリーID : cisco-sa-lnt-L9zOkBz5 CVE-2023-20135
初公開日 : 2023-09-13 16:00
バージョン 1.0 : Final
CVSSスコア : 5.7
回避策 : No workarounds available
Cisco バグ ID : CSCwd87928

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ソフトウェアイメージ検証チェックの脆弱性により、認証されたローカル攻撃者が基盤となるオペレーティングシステムで任意のコードを実行する可能性があります。

この脆弱性は、ISOイメージを使用するインストール操作中にISOイメージに関するインストールクエリが実行される際の、Time-of-Check, Time-of-Use(TOCTOU)競合状態に起因します。攻撃者は、ISOイメージを変更してからインストール要求を並行して実行することで、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で任意のコードを実行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-lnt-L9zOkBz5

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。これらのアドバイザリとそのリンクの一覧については、『Cisco Event Response: September 2023 Semiannual 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、これらの脆弱性は、Cisco IOS XRソフトウェアの脆弱性のあるリリースを実行し

ている次のシスコデバイスに影響を与えました。

- 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
- NCS5700イメージを実行しているNetwork Convergence System(NCS)5700シリーズルータ（NCS-57B1-5DSE-SYS、NCS-57B1-6D24-SYSおよびNCS-57C1-48Q6-SYS）

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。

ソフトウェアリリースの判別

デバイスで該当するソフトウェアイメージが実行されているかどうかを確認するには、デバイスのCLIでshow versionコマンドを使用します。次の例に示すように、出力にLNTが示されている場合、デバイスはこの脆弱性の影響を受けます。

```
<#root>

Router#

show version

Cisco IOS XR Software,

Version 7.5.2 LNT

Copyright (c) 2013-2022 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 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

発行時点では、次の表に記載されている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。

左の列はシスコソフトウェアリリースを示し、右の列はリリース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リリースを示しています。

Cisco IOS XR リリース	First Fixed Release（修正された最初のリリース）
7.5.2 より前	影響なし。
7.5.2 以降	修正済みリリースに移行。
7.6 以降	影響なし。
7.7 以降	7.10.1

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-lnt-L9zOkBz5

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	2023-9-13

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。