# Cisco IOS XRソフトウェアのCLIにおける特権昇格の脆弱性


アドバイザリーID : cisco-sa-iosxr-priv-esc-CrG5vhCq
CVE-2024-20398
初公開日 : 2024-09-11 16:00
バージョン 1.0 : Final
CVSSスコア : 8.8
回避策 : No workarounds available
Cisco バグ ID : CSCwj25248

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CLIにおける脆弱性により、認証されたローカル攻撃者が、該当デバイスの基盤となるオペレーティングシステムで読み取り/書き込み可能なファイルシステムアクセスを取得できる可能性があります。

この脆弱性は、特定のCLIコマンドに渡されるユーザ引数の検証が不十分であることに起因します。権限の低いアカウントを持つ攻撃者は、プロンプトで巧妙に細工されたコマンドを使用して、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 root に特権昇格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-iosxr-priv-esc-CrG5vhCq

このアドバイザリは、2024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。アドバイザリとリンクの一覧については、Cisco Event Response: September 2024 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

この脆弱性は、デバイス設定に関係なく、Cisco IOS XR 64ビットソフトウェアに影響を与えます。

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
- IOS XR 32 ビットソフトウェア
- 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

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示します。右の列は、リリース（トレイン）がこのアドバイザリに記載された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） |
|---|---|
| 7.11 以前 | 7.11.21（2024年10月） |
| 24.1 | 24.1.2 |
| 24.2 | 影響なし。 |

シスコはこの脆弱性に対処する次の SMU もリリースしています。一覧に記載されていないリリース向けの SMU を必要とするお客様は、サポート部門にご連絡ください。

| Cisco IOS XR ソフトウェア リリース | Platform | SMU 名 |
|---|---|---|
| 7.3.2 | ASR9K-X64<br>NCS540<br>NCS560<br>NCS5500 | asr9k-x64-7.3.2.CSCwk94350<br>ncs540-7.3.2.CSCwk94350<br>ncs560-7.3.2.CSCwk94350<br>ncs5500-7.3.2.CSCwk94350 |
| 7.5.2 | 8000 シリーズ<br>ASR9K-X64 | 8000-7.5.2.CSCwk94350<br>asr9k-x64-7.5.2.CSCwk94350 |

| Cisco IOS XR ソフトウェア リリース | Platform | SMU 名 |
|---|---|---|
| | NCS540<br>NCS540L<br>NCS560<br>NCS5500 | ncs540-7.5.2.CSCwk94350<br>ncs540l-7.5.2.CSCwk94350<br>ncs560-7.5.2.CSCwk94350<br>ncs5500-7.5.2.CSCwk94350 |
| 7.7.2 | 8000 シリーズ<br>ASR9K-X64 | 8000-7.7.2.CSCwk94350<br>asr9k-x64-7.7.2.CSCwk94350 |
| 7.8.2 | ASR9K-X64<br>NCS540<br>NCS5500 | asr9k-x64-7.8.2.CSCwk94350<br>ncs540-7.8.2.CSCwk94350<br>ncs5500-7.8.2.CSCwk94350 |
| 7.9.2 | 8000 シリーズ<br>ASR9K-X64<br>NCS5500 | 8000-7.9.2.CSCwk94350<br>asr9k-x64-7.9.2.CSCwk94350<br>ncs5500-7.9.2.CSCwk94350 |
| 7.9.21 | ASR9K-X64 | asr9k-x64-7.9.21.CSCwk94350 |
| 7.10.2 | 8000 シリーズ<br>ASR9K-X64<br>NCS560 | 8000-7.10.2.CSCwk94350<br>asr9k-x64-7.10.2.CSCwk94350<br>ncs560-7.10.2.CSCwk94350 |
| 7.11.2 | ASR9K-X84<br>NCS540<br>NCS540L<br>NCS5500<br>NCS5700 | asr9k-x64-7.11.2.CSCwk94350<br>ncs540-7.11.2.CSCwk94350<br>ncs540l-7.11.2.CSCwk94350<br>ncs5500-7.11.2.CSCwk94350<br>ncs5700-7.11.2.CSCwk94350 |

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

シスコは、この脆弱性を報告していただいたイタリアの国家サイバーセキュリティ機関(ACN)のFrancesco Caserta氏およびAlessandro Ruggieri氏に感謝いたします。

## URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-priv-esc-CrG5vhCq

## 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9月11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。