

# Cisco IOS XRソフトウェアのCLIにおける任意のファイル読み取りの脆弱性



アドバイザリーID : cisco-sa-iosxr-shellutil- [CVE-2024-](#)

HCb278wD

[20343](#)

初公開日 : 2024-09-11 16:00

バージョン 1.0 : Final

CVSSスコア : [5.5](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwi71881](#)

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、基盤となるLinuxオペレーティングシステムのファイルシステム内の任意のファイルを読み取る可能性があります。攻撃者は、影響を受けるデバイスに対する有効なログイン情報を有している必要があります。

この脆弱性は、特定のCLIコマンドに渡される引数の検証が正しく行われなことに起因します。攻撃者は、権限の低いクレデンシャルで該当デバイスにログインし、該当コマンドを使用することで、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Linuxファイルシステム上の読み取り専用モードでファイルにアクセス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。

このアドバイザリーは、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-shellutil-HCb278wD>

このアドバイザリーは、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ーバンドルの一部です。アドバイザリー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

公開時点では、デバイスの設定にかかわらず、この脆弱性はCisco IOS XR 64ビットソフトウェアに影響を与えていました。

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
- 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

[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

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<br>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                        | 7.11.2                               |
| 24.1                        | 24.1.2                               |
| 24.2                        | 影響なし。                                |

このドキュメントの発行時点で、シスコはこの脆弱性に対処するために次のSMUをリリースしました。SMUの可用性を含む最新の情報を含む最も完全な情報については、このアドバイザリの上部にあるバグIDの詳細情報のセクションを参照してください。一覧に記載されていないプラットフォームやリリース向けの 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<br>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<br>NCS540<br>NCS540L<br>NCS560<br>NCS5500 | 8000-7.5.2.CSCwk94350<br>asr9k-x64-7.5.2.CSCwk94350<br>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                                   | asr9k-x64-7.11.2.CSCwk94350<br>ncs540-7.11.2.CSCwk94350<br>ncs540l-7.11.2.CSCwk94350  |

| Cisco IOS XR ソフトウェア<br>リリース | Platform           | SMU 名  |
|-----------------------------|--------------------|--|
|                             | NCS5500<br>NCS5700 | 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Bip ConsultingのAlberto Crosta氏に感謝いたしま  
す。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-shellutil-HCb278wD>

## 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

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものでは  
ありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者に  
あるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したり  
する権利を有します。

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、  
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。