# Cisco IOS XRソフトウェアの認証されたCLIセキュアコピープロトコルおよびSFTPにおけるDoS脆弱性

Medium

アドバイザリーID : cisco-sa-iosxr-scp-dos-kb6sUUHw
CVE-2024-20262
初公開日 : 2024-03-13 16:00
バージョン 1.0 : Final
CVSSスコア : 6.5
回避策 : No workarounds available
Cisco バグ ID : CSCwf11720

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Secure Copy Protocol(SCP)およびSFTP機能の脆弱性により、認証されたローカル攻撃者がシステムディレクトリでファイルを作成または上書きすることが可能になり、サービス妨害(DoS)状態が発生する可能性があります。攻撃者がこの攻撃を実行するには、有効なユーザクレデンシャルが必要です。

この脆弱性は、SCPおよびSFTP CLI入力パラメータの適切な検証が行われないことに起因します。攻撃者は、デバイスに認証され、特定のパラメータを指定してSCPまたはSFTP CLIコマンドを発行することにより、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、攻撃者はデバイスの機能に影響を与え、DoS状態を引き起こす可能性があります。回復するには、デバイスを手動で再起動する必要がある場合があります。

注：この脆弱性が不正利用できるのは、ローカルユーザがCisco IOS XR CLIでSCPまたはSFTPコマンドを呼び出した場合だけです。管理権限を持つローカルユーザが、この脆弱性をリモートから不正利用す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-scp-dos-kb6sUUHw

このアドバイザリは、2024年3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: March 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、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シスコデバイスに影響を与えました。この脆弱性は、デフォルトで有効になっているSCPおよびSFTP機能に関連しています。

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。

ただし、この脆弱性はCisco IOS XR CLIでSCPまたはSFTPコマンドを呼び出すローカルユーザによってのみ不正利用が可能であるため、認証、許可、アカウンティング(AAA)コマンド許可を使用してscp およびsftp CLIコマンドをブロックしたり、scp およびsftp コマンドを信頼できるユーザだけが使用したりできます。詳細については、『Cisco IOS XRソフトウェアでのAAAサービスの設定』の「AAA認証の有効化」セクションを参照してください。上記のように、この脆弱性は管理権限を持つユーザによってリモートで不正利用されます。

この緩和策は導入されており、テスト環境では実証済みですが、お客様は、ご使用の環境および使用条件において適用性と有効性を判断する必要があります。また、導入されている回避策または緩和策が、お客様固有の導入シナリオおよび制限に基づいて、ネットワークの機能やパフォーマンスに悪影響を及ぼす可能性があることに注意してください。回避策や緩和策は、ご使用の環境への適用性と環境への影響を評価した後で導入してください。

# 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。

左側の列にはシスコソフトウェアリリース、右側の列に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が示されています。

| 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） |
|---|---|
| 7.9 以前 | 修正済みリリースに移行。 |
| 7.10 | 修正済みリリースに移行。 |
| 7.11 | 7.11.1 |
| 24.1 | 24.1.1 |

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-iosxr-scp-dos-kb6sUUHw

## 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3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。