

Cisco IOS XRソフトウェアのSSHにおける特権昇格の脆弱性



アドバイザリーID : cisco-sa-iosxr-ssh-

privesc-eWDMKew3

初公開日 : 2024-03-13 16:00

バージョン 1.0 : Final

CVSSスコア : [7.8](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwh52374](#)

[CVE-2024-20320](#)

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 8000シリーズルータおよびCisco Network Convergence System(NCS)540シリーズおよび5700シリーズルータ用Cisco IOS XRソフトウェアのSSHクライアン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の特権を昇格できる可能性があります。

この脆弱性は、SSHクライアントCLIコマンドに含まれる引数の検証が不十分であることに起因します。該当デバイスへの低特権アクセスを持つ攻撃者は、CLIに巧妙に細工されたSSHクライアントコマンドを発行することにより、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権限をrootに昇格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-ssh-privesc-eWDMKew3>

このアドバイザリーは、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ーバンドルの一部です。アドバイザリーの全リストとそのリンクについては、『[Cisco Event Response: Seemannal 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、Cisco IOS XR ソフトウェアの脆弱性が存在す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す。

- 8000 シリーズ ルータ
- IOS XRdコントロールプレーン
- IOS XRd vRouter
- NCS540L イメージを実行している NCS 540 シリーズ ルータ
- NCS 5700シリーズルータ(NCS-57B1-5DSE-SYS、NCS-57B1-6D24-SYS、NCS-57C1-48Q6-SYS)

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。

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と表示されている場合、その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、緩和策として、コマンド許可を提供するようにAuthentication, Authorization, and Accounting (AAA ; 認証、認可、アカウンティング) サービスを設定している場合は、AAAサーバで定義されている許可ポリシーのsshコマンドへのアクセスを制限できます。

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

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することになります。

<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です。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を記載しています。右側の列は、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最初のリリースを示しています。このセクションの表に記載されている適切な [修正済みソフトウェアリリース](#) にアップグレードすることをお勧めします。

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)
7.3.2	修正済みリリースに移行。
7.4	修正済みリリースに移行。
7.5	修正済みリリースに移行。
7.6	修正済みリリースに移行。
7.7	修正済みリリースに移行。
7.8	修正済みリリースに移行。
7.9	修正済みリリースに移行。
7.10	7.10.2

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-ssh-privesc-eWDMKew3>

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

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。