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-privesc-bF8D5U4W
初公開日 : 2026-03-11 16:00
バージョン 1.0 : Final
CVSSスコア : 8.8
回避策 : Yes
Cisco バグ ID : CSCwp33021 CSCwp84685 CSCwp33030 CSCwp87543 CSCwp30142 CSCwp33034 CSCwp30135 CSCwp30146 CSCwp30149 CSCwp35627 CSCwp32614 CSCws24696 CSCws24740 CSCwp32629 CSCwp27221 CSCws24717

CVE-2026-20040
CVE-2026-20046

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ソフトウェアに存在する複数の脆弱性により、認証されたローカルの攻撃者が、基盤となるオペレーティングシステムでrootとしてコマンドを実行したり、影響を受けるデバイスの完全な管理制御を取得したりする可能性があります。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコはこれら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。これらの脆弱性の1つに対しては回避策があります。

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-privesc-bF8D5U4W

このアドバイザリは、Cisco IOS XRソフトウェアSecurity Advisoryバンドル公開の2026年3月リリースの一部です。アドバイザリとリンクの一覧については、Cisco Event Response: March 2026 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

CVE-2026-20040で説明されている脆弱性は、デバイス設定に関係なく、Cisco IOS XRソフトウェアに影響を与えます。

CVE-2026-20046で説明されている脆弱性は、デバイス設定に関係なく、Cisco IOS XRv 9000ルータに影響を与えます。

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、これら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

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために、他の脆弱性をエクスプロイトする必要はありません。また、いずれかの脆弱性の影響を受けるリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2026-20040:Cisco IOS XRソフトウェアのCLIにおける特権昇格の脆弱性

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任意のコマンドを root として実行できるようになります。

この脆弱性は、特定の CLI コマンドに渡されるユーザー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、攻撃者は権限をrootに昇格し、基盤となるオペレーティングシステムで任意のコマン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。

バグID(s): CSCwp84685、CSCwp27221、CSCwp30135、CSCwp33034、CSCws24740、CSCws24717、CSCwp33021、CSCwp326 4、CSCwp30142、CSCws24696、CSCwp30149、CSCwp35627、CSCwp32629、CSCwp30146、CSCwp33030
CVE ID：CVE-2026-20040
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.8
CVSS ベクトル：CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVE-2026-20046:Cisco IOS XRソフトウェアのCLIにおける特権昇格の脆弱性

Cisco IOS XRソフトウェアの特定のCLIコマンドに対するタスクグループ割り当ての脆弱性により、認証されたローカルの攻撃者が権限を昇格させ、該当デバイスの完全な管理制御を取得する可能性があります。

この脆弱性は、ソースコード内のタスクグループへのコマンドのマッピングが不適切なことに起因します。権限の低いアカウントを持つ攻撃者は、CLIコマンドを使用してタスクグループベースのチェックをバイパスすることにより、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、攻撃者は権限を昇格させ、権限チェックを行わずに該当デバイスでアクション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。本脆弱性に対処する回避策がいくつかあります。

バグID: CSCwp87543
CVE ID：CVE-2026-20046
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：8.8
CVSS ベクトル：CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

回避策

CVE-2026-20040:この脆弱性に対処する回避策はありません。

CVE-2026-20046:TACACS+ authentication, authorization, and accounting(AAA)コマンド許可が設定されているデバイスに対してのみ、回避策があります。管理者はこの機能を使用して、非管理者ユーザが必要とするコマンドへのアクセスのみを許可し、他のすべてのコマンドへのアクセスを拒否できます。

この回避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

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。これらの脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

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。中央および右の列は、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、およびこれら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	CVE-2026-20040 の最初の修正済みリリース	CVE-2026-20046 の最初の修正済みリリース
25.1 以前	修正済みリリースに移行。	修正済みリリースに移行。
25.2	25.2.21（2026年3月）	25.2.2
25.3	修正済みリリースに移行。	影響なし。
25.4	25.4.2（2026年3月）	影響なし。
26.1	影響なし。	影響なし。

これらの脆弱性に対処するためにSMUも使用できます。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。これらの脆弱性に対して公開されている可能性があるSMUを見つける方法の詳細については、『Cisco IOS XRソフトウェアメンテナンスアップデート(SMU)について』の「ダウンロード」セクションを参照してください。

注：Cisco Bug ID CSCws61542のSMUにはCSCwp30135とCSCws24717の修正が含まれています。Cisco Bug ID CSCws35777のSMUには、CSCwp33034の修正が含まれています。

シスコの 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済み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とその公表は確認し

ておりません。

出典

CVE-2026-20040：この脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のTristan Van Egrooによる内部セキュリティテストで発見されました。

CVE-2026-20046：この脆弱性は、内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-privesc-bF8D5U4W

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	2026年3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。