

Cisco IOS XE ソフトウェアにおける特権昇格の脆弱性 (複数)



アドバイザーID : [cisco-sa-iosxe-privesc-su7scvdp](#) [CVE-2025-20197](#)
初公開日 : 2025-05-07 16:00 [CVE-2025-20198](#)
バージョン 1.0 : Final [CVE-2025-20199](#)
CVSSスコア : [6.7](#) [CVE-2025-20200](#)
回避策 : No workarounds available [CVE-2025-20201](#)
Cisco バグ ID : [CSCwm59330](#)
[CSCwm66565](#) [CSCwm68661](#)
[CSCwm72787](#) [CSCwm64309](#)

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 XEソフトウェアのCLIにおける複数の脆弱性により、特権レベル15を持つ認証されたローカルの攻撃者が、該当デバイスの基盤となるオペレーティングシステム上で権限をルートに昇格させる可能性があります。

これらの脆弱性は、特定の設定コマンドを処理する際の入力検証が不十分であることに起因します。攻撃者は、巧妙に細工された入力を特定の設定コマンドに含めることによって、これら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、該当デバイスの基盤となるオペレーティングシステムでルートとして特権を昇格できるようになります。攻撃者が影響を受けるデバイスの基盤となるオペレーティングシステムにアクセスし、検出されない可能性のあるアクションを実行する可能性があるため、このアドバイザリのSecurity Impact Rating(SIR)は「High」に格上げされました。

注：攻撃者は該当するデバイスでコンフィギュレーションモードに入る権限を持っている必要があります。これは通常、特権レベル15と呼ばれます。

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-iosxe-privesc-su7scvdp>

このアドバイザリは、2025年5月に公開されたCisco IOSソフトウェアおよびIOS XEソフトウェアのセキュリティアドバイザリバンドルの一部です。これらのアドバイザリとリンクの一覧については、『[シスコイベントレスポンス：Cisco IOSおよびIOS XEソフトウェアに関するセキュリティアドバイザリ公開資料（半年刊、2025年5月）](#)』を参照してください。

該当製品

脆弱性のある製品

これらの脆弱性は、デバイス設定に関係なく、Cisco IOS XEソフトウェアの脆弱性のあるリリースを実行するシスコ製品に影響を与えます。

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 XR ソフトウェア
- Meraki 製品
- NX-OS ソフトウェア

回避策

これら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ン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完全なアップグレード ソリューション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。

Cisco IOS および IOS XE ソフトウェア

お客様が Cisco IOS および IOS XE ソフトウェアの脆弱性による侵害の可能性を判断できるように、シスコは [Cisco Software Checker](#) を提供しています。このツールを使うことで、特定のソフトウェアリリースに関連するすべてのシスコ セキュリティ アドバイザリを検索でき、それぞれのアドバイザリで言及された脆弱性を修正した最初のリリース (「First Fixed」) を特定できます。また、該当する場合には、Software Checker により判別されたすべてのアドバイザリに記載のすべての脆弱性が修正された最初のリリース (「Combined First Fixed」) を特定できます。

このツールを使用するには、「[Cisco Software Checker](#)」ページの手順に従います。あるいは、次のフォームを使用して、シスコ セキュリティ アドバイザリに該当するリリースであるかどうかを確認します。このフォームを使用するには、次の手順に従います。

1. ツールで検索するアドバイザリを選択します。このアドバイザリのみ、[セキュリティ影響評](#)

[価値 \(SIR\)](#) が「重大」または「高」のアドバイザリのみ、すべてのアドバイザリのいずれかです。

2. リリース番号 (例: 15.9(3)M2、17.3.3) を入力します。

3. [チェック (Check)] をクリックします。

2		Critical,High,Medium
このアドバイザのみ		
Enter release number	Check	

不正利用事例と公式発表

Cisco Product Security Incident Response Team(PSIRT)では、本アドバイザリに記載されている脆弱性のエクスプロイト事例とその公表は確認しておりません。

出典

これらの脆弱性は、Cisco Advanced Security Initiatives Group(ASIG)のT.V.およびX.B.によって、内部でのセキュリティテスト中に発見されました。

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-privesc-su7scvdp>

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	2025年5月7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。