

Cisco IOS XEソフトウェアのモデル駆動型プログラマビリティにおける認証バイパスの脆弱性



アドバイザリーID : cisco-sa-netconf-nacm- [CVE-2025-bypass-TGZV9pmQ](#) [20214](#)

初公開日 : 2025-05-07 16:00

バージョン 1.0 : Final

CVSSスコア : [4.3](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCwi33204](#)

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Network Configuration Access Control Module(NACM)における脆弱性により、認証されたりモート攻撃者が、構成データまたは運用データに対する不正な読み取りアクセスを取得できる可能性があります。

この脆弱性は、内部APIコールの動作が微妙に変更されたために、結果が正しくフィルタリングされないことに起因しています。攻撃者は、NETCONF、RESTCONF、またはgRPCネットワーク管理インターフェイス(gNMI)プロトコルのいずれかを使用して、NACM設定によって拒否された可能性のあるパスのデータを照会することで、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、NACM設定に従って制限されているべきデータにアクセスできる可能性があります。

注 : この脆弱性を悪用するには、攻撃者が15より低い権限を持つ有効なユーザからクレデンシャルを取得し、NACMがそのユーザに制限付き読み取りアクセスを提供するように設定されている必要があります。

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-netconf-nacm-bypass-TGZV9pmQ>

このアドバイザリーは、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ーバンドルの一部です。これらのアドバイザリー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ー公開資料 \(半年刊、2025年5月 \)](#)』を参照してください。

該当製品

脆弱性のある製品

公開時点では、この脆弱性の影響を受けたシスコデバイスで脆弱性が存在するCisco IOS XEソフトウェアリリースを実行していて、さらに権限の低いユーザに対して制限された読み取りアクセスを提供するNACMポリシーが有効にされている場合、この脆弱性の影響を受けます。

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](#)にリストされている製品だけがこの脆弱性の影響を受けることが知られています。

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 XR ソフトウェア
- Meraki 製品
- 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。

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 \(SIR\)](#) 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）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を確認していません。

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-netconf-nacm-bypass-TGZV9pmQ>

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。