Cisco IOS XE ソフトウェアの SNMP サービス妨害（DoS）の脆弱性

アドバイザリーID : cisco-sa-iosxe-snmp-dos-ZAqNm4MD
初公開日 : 2026-08-05 16:00
バージョン 1.0 : Final
CVSSスコア : 7.7
回避策 : No workarounds available
Cisco バグ ID : CSCws90638

CVE-2026-20124

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Simple Network Management Protocol(SNMP)サブシステムの脆弱性により、認証されたリモート攻撃者が該当デバイスのリロードを引き起こし、その結果、サービス妨害(DoS)状態が発生する可能性があります。

この脆弱性は、SNMP リクエストを解析するときのエラー処理が適切でないことに起因します。この脆弱性は、SNMPのすべてのバージョン（バージョン1、2c、および3）に影響します。攻撃者は、該当デバイスに不正なSNMP要求を送信することで、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、攻撃者はデバイスの予期しないリロードを引き起こすことができるようになります。攻撃者は、該当するデバイスで、SNMPv1かv2cの読み取り専用コミュニティストリングか読み取りと書き込みコミュニティストリング、または有効なSNMPv3ユーザクレデンシャルを持っている必要があります。

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。この脆弱性に対処する緩和策があります。

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-iosxe-snmp-dos-ZAqNm4MD

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOS XEソフトウェアの脆弱性が存在するリリースを実行し、SNMPを有

効にしているシスコデバイスに影響を与えます。

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。

デバイス設定の確認

デバイスで SNMPv1 または v2c が有効になっているかどうかを確認するには、show running-config | include snmp-server community CLI コマンドを使用します。次の例に示すように、出力がある場合は、SNMP が有効になっています。

```
<#root>

Router#

show running-config | include snmp-server community


snmp-server community public ro
```

デバイスで SNMPv3 が有効になっているかどうかを確認するには、show running-config | include snmp-server group and show snmp user CLI コマンドを使用します。次の例に示すように、両方のコマンドの出力がある場合、SNMPv3 が有効になっています。

```
<#root>

Router#

show running-config | include snmp-server group


snmp-server group v3group v3 noauth

Router#

show snmp user


User name: remoteuser1
Engine ID: 800000090300EE01E71C178C
storage-type: nonvolatile     active
Authentication Protocol: SHA
Privacy Protocol: None
Group-name: v3group
```

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
- 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、緩和策があります。管理者は、デバイス上で影響を受ける OID を無効にすることができます。すべてのソフトウェアが軽減策に記載されている OID をサポートしているわけではありません。OID が特定のソフトウェアに対して有効でない場合、この脆弱性の影響を受けません。これらの OID を除外すると、ディスカバリやハードウェアインベントリなど、SNMP を介したデバイス管理に影響する可能性があります。

ビューエントリを作成または更新して、影響を受ける OID を無効にするには、次の例に示すように、snmp-server view グローバル コンフィギュレーション コマンドを使用します。

```
!Standard VIEW and Security Exclusions
snmp-server view NO_BAD_SNMP iso included
snmp-server view NO_BAD_SNMP snmpUsmMIB excluded
snmp-server view NO_BAD_SNMP snmpVacmMIB excluded
snmp-server view NO_BAD_SNMP snmpCommunityMIB excluded
!End Standard View

!Advisory Specific Mappings
!CISCO-IETF-DHCP-SERVER-MIB Subnet Information
snmp-server view NO_BAD_SNMP cDhcpv4ServerSubnetMask excluded
snmp-server view NO_BAD_SNMP cDhcpv4ServerSubnetSharedNetworkName excluded
snmp-server view NO_BAD_SNMP cDhcpv4ServerSubnetFreeAddrLowThreshold excluded
snmp-server view NO_BAD_SNMP cDhcpv4ServerSubnetFreeAddrHighThreshold excluded
snmp-server view NO_BAD_SNMP cDhcpv4ServerSubnetFreeAddresses excluded
snmp-server view NO_BAD_SNMP cDhcpv4ServerSubnetStartAddress excluded
snmp-server view NO_BAD_SNMP cDhcpv4ServerSubnetEndAddress excluded
!End Advisory Specific Mappings
```

その後、コミュニティストリングにこのコンフィギュレーションを適用するため、次のコマンドを使用します。

```
snmp-server community mycomm view NO_BAD_SNMP RO
```

SNMPv3 の場合は、次のコマンドを使用します。

```
snmp-server group v3group v3 auth read NO_BAD_SNMP write NO_BAD_SNMP
```

Meraki クラウド管理型スイッチをご使用のお客様：ダッシュボード組織のデバイスで該当ソフトウェアリリースが稼働している場合は、Meraki サポートチームに連絡し、修正済みソフトウェアが入手可能になるまで推奨される緩和策を適用してください。

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。

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

この脆弱性を報告してくださった外部の研究者に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-snmp-dos-ZAqNm4MD

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 8 月 5 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。