Cisco IOSおよびIOS XEソフトウェアのSNMPにおけるサービス妨害(DoS)およびリモートコード実行の脆弱性

アドバイザリーID : cisco-sa-snmp-x4LPhte
初公開日 : 2025-09-24 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 : CSCwq31287
CVE-2025-20352

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ソフトウェアおよび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、次の問題が発生する可能性があります。

- 権限の低い認証されたリモート攻撃者が、Cisco IOSソフトウェアまたはCisco IOS XEソフトウェアを実行する該当デバイスでサービス妨害(DoS)状態を引き起こす可能性があります。DoSを引き起こすには、攻撃者はSNMPv2c以前の読み取り専用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。
- 高い権限を持つ認証されたリモートの攻撃者が、Cisco IOS XEソフトウェアを実行する影響を受けるデバイスでrootユーザとしてコードを実行する可能性があります。攻撃者がrootユーザとしてコードを実行するには、該当デバイスで、SNMPv1またはv2cの読み取り専用コミュニティストリング、あるいは有効なSNMPv3ユーザクレデンシャルと、管理者クレデンシャル、または特権15のクレデンシャルを持っている必要があります。

攻撃者は、IPv4またはIPv6ネットワークを介して該当デバイスに巧妙に細工されたSNMPパケットを送信することにより、この脆弱性を不正利用する可能性があります。

この脆弱性は、該当ソフトウェアのSNMPサブシステムにおけるスタックオーバーフロー状態に起因します。エクスプロイトが成功すると、権限の低い攻撃者が該当システムのリロードを引き起こし、その結果DoS状態が発生する可能性があります。または、権限の高い攻撃者がルートユーザとして任意のコードを実行し、該当システムのフルコントロールを取得する可能性があります。

注：この脆弱性は、すべてのバージョンのSNMPに影響します。

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ました。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-snmp-x4LPhte

このアドバイザリは、Cisco IOS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公開の2025年9月リリースの一部です。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9月）』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ソフトウェアまたは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デバイスに影響を与えます。

Meraki CS 17以前を実行しているMeraki MS390およびCisco Catalyst 9300シリーズスイッチも該当します。これは、Cisco IOS XEソフトウェアリリース17.15.4aで修正されています。

注：この脆弱性は、すべてのバージョンのSNMPに影響します。SNMPが有効で、影響を受けるオブジェクトID(OID)を明示的に除外していないデバイスはすべて、脆弱であると見なされます。OIDの除外の詳細については、このアドバイザリの「回避策」セクションを参照してください。

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
```

特定のデバイスで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およびshow snmp user CLIコマンドを使用します。両方のコマンドの出力がある場合は、次の例に示すように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 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。

信頼できるユーザだけに SNMP アクセスを許可することが推奨されます。また、CLI で show snmp host コマンドを使用して該当システムをモニタすることも推奨されます。

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。この緩和策でリストされているOIDは、すべてのソフトウェアでサポートされ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該当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-AUTH-FRAMEWORK-MIB
snmp-server view NO_BAD_SNMP cafSessionMethodsInfoEntry.2.1.111 excluded
```

この設定をコミュニティストリングに適用するには、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 auth read NO_BAD_SNMP write NO_BAD_SNMP
```

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、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、回避策や緩和策は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復し、本アドバイザリで説明されている障害の発生を回避するために、お客様には本アドバイザリで説明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、ローカルの管理者クレデンシャルが侵害された後、この脆弱性が悪用されると認識しました。この脆弱性を修正するために、修正済みのソフトウェアリリースにアップグレードすることを強くお勧めします。

出典

この脆弱性は、Cisco Technical Assistance Center(TAC)のサポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte

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9月24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、単独の転載や意訳を施した場合、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。