Cisco IOS XEソフトウェアのSimple Network Management Protocolにおける Denial of Service(DoS)の脆弱性

アドバイザリーID : cisco-sa-snmpwred-x3MJyf5M
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 : Yes
Cisco バグ ID : CSCwp03900

CVE-2025-20312

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にサービス妨害(DoS)状態を引き起こす可能性があります。

この脆弱性は、特定のSNMP要求を解析する際の不適切なエラー処理に起因します。攻撃者は、該当デバイスに特定のSNMP要求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。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可能になり、結果として DoS 状態が発生する可能性があります。

この脆弱性は、SNMP バージョン 1、2c、および 3 に影響します。SNMPv2c以前のバージョンでこの脆弱性をエクスプロイトするには、攻撃者が該当システムの有効な読み取り/書き込み可能または読み取り専用SNMPコミュニティストリングを知っている必要があります。SNMPv3を介してこの脆弱性をエクスプロイトするには、攻撃者が該当システムの有効なSNMP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。ただし、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-snmpwred-x3MJyf5M

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 XEソフトウェアの脆弱性が存在するリリースを実行し、マルチプロトコルラベルスイッチング(MPLS)のWeighted Early Random Detection(WRED)Experimental Field(EXP)が設定され、SNMP機能が有効になっているシスコスイッチに影響を与えます。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。

注：Cisco IOS XEソフトウェアを実行するシスコのルーティングプラットフォームは、MPLS EXPに対するWREDをサポートしていないため、この脆弱性の影響を受けません。

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。

MPLS EXP設定のWREDの判別

デバイスでMPLS EXPのWREDが設定されているかどうかを確認するには、show running-config CLIコマンドを使用し、適用されているポリシーにrandom-detect mpls-exp-basedコマンドが存在するかどうかを確認します。出力があり、そのクラスが適用されたポリシーマップの一部である場合（次の例を参照）、そのデバイスは脆弱であると見なされます。

```
<#root>

Switch#

show running-config


policy-map TEST
 class class-default


random-detect mpls-exp-based


!
interface GigabitEthernet 1/0/48
 service-policy output TEST
```

デバイスでMPLS EXPのWREDが設定されていない場合、この脆弱性の影響を受けません。

SNMP 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>

Switch#

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>

Switch#

show running-config | include snmp-server group


snmp-server group v3group v3 noauth

Switch#

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、管理者は緩和策として、デバイスの脆弱なオブジェクト識別子(OID)を無効にすることができます。

影響を受けるOIDの無効化

ベストプラクティスとして、SNMP アクセスを信頼できるネットワークデバイスからのみ許可する必要があります。設定オプションについては、「Simple Network Management Protocol の保護」を参照してください。

OIDを無効にするには、次の手順に従います。

1. 標準セキュリティ設定で SNMP ビューを作成します。

```
snmp-server view SNMP_DOS iso included
snmp-server view SNMP_DOS snmpUsmMIB excluded
snmp-server view SNMP_DOS snmpVacmMIB excluded
snmp-server view SNMP_DOS snmpCommunityMIB excluded
```

2. SNMPビューから脆弱なOIDを除外します。

```
snmp-server view SNMP_DOS cbQosREDClassStatsEntry excluded
```

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、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-snmpwred-x3MJyf5M

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。