Cisco IOS XE SD-WANソフトウェアのパケットフィルタリングバイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-snmp-bypass-HHUVujdn　CVE-2025-20221
初公開日 : 2025-05-07 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : Yes
Cisco バグ ID : CSCwn25087

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 SD-WANソフトウェアのパケットフィルタリング機能の脆弱性により、認証されていないリモートの攻撃者がレイヤ3およびレイヤ4トラフィックフィルタをバイパスできる可能性があります。

この脆弱性は、該当デバイスでの不適切なトラフィックフィルタリング条件に起因します。攻撃者は、巧妙に細工されたパケットを該当デバイスに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、攻撃者はレイヤ3およびレイヤ4トラフィックフィルタをバイパスし、巧妙に細工されたパケットをネットワークに挿入できる可能性があります。

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。本脆弱性に対処する回避策がいくつかあります。

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-bypass-HHUVujdn

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

Cisco IOS XE ソフトウェア

公開時点では、この脆弱性は、コントローラモードで実行されているユニバーサルCisco IOS XEソフトウェアリリース17.2.1r以降に影響を与えました。Cisco IOS XEソフトウェアリリース17.2.1rより前のリリースにはSD-WAN機能が含まれていないため、この脆弱性の影響を受けません。

公開時点では、この脆弱性は次のスタンドアロンCisco IOS XE SD-WANソフトウェアリリースにも影響を与えました。

- 16.9.1 ~ 16.9.4
- 16.10.1 ~ 16.10.5
- 16.11.1a
- 16.12.2r ~ 16.12.4

注：スタンドアロンのCisco IOS XE SD-WANリリースイメージは、ユニバーサルCisco IOS XEソフトウェアリリースとは別のものです。SD-WAN機能セットは、Cisco IOS XEソフトウェアリリース17.2.1r以降のユニバーサルCisco IOS XEソフトウェアリリースに最初に統合されました。詳細については、『Cisco Catalyst SD-WANスタートアップガイド』の「Cisco IOS XE Catalyst SD-WANリリース17.2.1r以降のインストールとアップグレード」の章を参照してください。

Cisco IOS XE cEdgeルータ

この脆弱性の公開時点では、トンネル0インターフェイスでSimple Network Management Protocol(SNMP)が有効になっているCisco SD-WAN cEdgeルータに影響が及んでいました。SNMPが有効になっていない場合、デバイスはこの脆弱性の影響を受けません。

このアドバイザリの公開時点で脆弱性が存在するシスコ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

特定のデバイスでSNMPバージョン1(SNMPv1)またはコミュニティベースのSNMPバージョン2(SNMPv2c)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。

```
Router# show running-config | include snmp-server community
snmp-server community public ro
```

デバイスでSNMPバージョン3(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。

```
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
- Meraki
- 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。

この問題を解決するには、Cisco SD-WAN Managerインターフェイスから次のいずれかの変更を行います。

- デバイスとの間で送受信される特定の入力トラフィックと出力トラフィックをブロックおよび許可するように、拡張アクセスコントロールリスト(ACL)を設定します。手順については、「vManageポリシーを使用してcEdge上のトラフィックをブロック/一致させるためのACLの設定」を参照してください。
- 未承諾のSNMPトラフィックをブロックするために、デバイスアクセスポリシーをエッジデバイスにプッシュするように設定します。ポリシーを設定する際は、要求を送信するホストに応答が送信される前にSNMPv3認可が実行される必要があることを考慮してください。

手順については、『Cisco Catalyst SD-WANポリシーコンフィギュレーションガイド』の「デバイスアクセスポリシー」の章を参照してください。

デバイスがコントローラモードでない場合、またはデバイスでSD-WANが有効になっていない場合、そのデバイスはこの脆弱性の影響を受けません。

この回避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

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、アドバイザリで説明されている脆弱性に対して概念実証段階のエクスプロイト コードが入手可能であることを認識しています。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

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-snmp-bypass-HHUVujdn

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

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。