Cisco IOS、IOS XE、およびIOS XRソフトウェアのSNMPにおけるDenial of Service(DoS)の脆弱性

アドバイザリーID : cisco-sa-snmp-dos-sdxnSUcW
初公開日 : 2025-02-05 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 : CSCwm89600 CSCwm79577 CSCwm79564 CSCwm79554 CSCwm79596 CSCwn08493 CSCwm79570 CSCwm79581 CSCwm79590

CVE-2025-20170
CVE-2025-20171
CVE-2025-20172
CVE-2025-20173
CVE-2025-20174
CVE-2025-20175
CVE-2025-20176
CVE-2025-20169

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、Cisco IOS XEソフトウェア、およびCisco IOS XRソフトウェアのSimple Network Management Protocol(SNMP)サブシステムにおける複数の脆弱性により、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。

これらの脆弱性の詳細については本アドバイザリの「詳細情報」セクションを参照してください。

シスコでは、これら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する予定です。これらの脆弱性に対処する回避策はありません。これらの脆弱性に対処する対応策があります。

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-

dos-sdxnSUcW

該当製品

脆弱性のある製品

これらの脆弱性は、Cisco IOSソフトウェア、Cisco IOS XEソフトウェア、またはSNMP機能を有効にしたCisco IOS XRソフトウェアの脆弱性のあるリリースを実行しているシスコデバイスに影響を与えます。これらの脆弱性は、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。

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SNMP v1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-configuration | include snmp-server community CLIコマンドを使用します。出力がある場合は、次の例に示すように、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SNMP v3が有効になっているかどうかを確認するには、show running-configuration | 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、SNMP v3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が存在する製品セクションにリストされている製品だけがこれらの脆弱性の影響を受けることが知られています。

詳細

これらの脆弱性は依存関係にはなく、いずれかの脆弱性をエクスプロイトするために別の脆弱性をエクスプロイトする必要はありません。さらに、いずれかの脆弱性の影響を受けるソフトウェアリリースであっても、他の脆弱性の影響は受けない場合があります。

脆弱性の詳細は以下のとおりです。

CVE-2025-20169、CVE-2025-20170、CVE-2025-20171、CVE-2025-20173、CVE-2025-20174、CVE-2025-20175、CVE-2025-20176:Cisco IOSおよびIOS XEソフトウェアのSNMPソフトウェアにおけるDoS脆弱性

Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアのSNMPサブシステムにおける複数の脆弱性により、認証されたリモート攻撃者が該当デバイスにDoS状態を引き起こす可能性があります。

これらの脆弱性は、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、該当デバイスに巧妙に細工されたSNMP要求を送信することにより、これら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。

これらの脆弱性は、SNMPバージョン1、2c、および3に影響を与えます。SNMP v2c以前のバージョンでこれら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。SNMP v3でこれら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。

シスコでは、これら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する予定です。これらの脆弱性に対処する回避策はありません。これらの脆弱性に対処する対応策があります。

バグID(s): CSCwm79581、CSCwm79554、CSCwm79564、CSCwm79590、CSCwm79570、CSCwm79596、CSCwm79577
CVE ID:CVE-2025-20169、CVE-2025-20170、CVE-2025-20171、CVE-2025-20173、CVE-2025-

20174、CVE-2025-20175、CVE-2025-20176
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.7
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

CVE-2025-20172:Cisco IOS、IOS XE、およびIOS XRソフトウェアのSNMPにおけるDoS脆弱性

Cisco IOSソフトウェア、Cisco IOS XEソフトウェア、およびCisco IOS XRソフトウェアのSNMPサブシステムにおける脆弱性により、認証されたリモート攻撃者が該当デバイスにDoS状態を引き起こす可能性があります。

この脆弱性は、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、巧妙に細工された SNMP 要求を該当デバイスに送信することにより、この脆弱性をエクスプロイトする可能性があります。Cisco IOSおよびIOS XEソフトウェアでは、エクスプロイトに成功すると、攻撃者がデバイスの予期しない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。Cisco IOS XRソフトウェアの場合、エクスプロイトに成功すると、攻撃者はSNMPプロセスを再起動させ、影響を受けるデバイスからSNMP応答が中断される可能性があります。Cisco IOS XRソフトウェアを実行しているデバイスはリロードされません。

この脆弱性は、SNMPバージョン1、2c、および3に影響します。SNMP v2c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。SNMP v3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。

シスコでは、これら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する予定です。これらの脆弱性に対処する回避策はありません。これらの脆弱性に対処する対応策があります。

Cisco IOS および IOS XE ソフトウェア

バグID: CCSCwm89600
CVE ID:CVE-2025-20172
セキュリティ影響評価（SIR）：高
CVSS ベーススコア：7.7
CVSSベクトル：CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

Cisco IOS XR ソフトウェア

バグID: CSCwn08493
CVE ID:CVE-2025-20172
セキュリティ影響評価（SIR）：中
CVSS ベーススコア：4.3
CVSSベクトル： CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L

回避策

これらの脆弱性に対処する回避策はありません。ただし、対応策があります。修正済みソフトウェアが利用可能になり、アップグレードが実行できるようになるまで、これらの緩和策を実装することを強く推奨します。

管理者は、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。この緩和策に記載されている各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、その特定の脆弱性に対して脆弱ではありません。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によるデバイス管理に影響を与える可能性があります。

ベストプラクティスとして、SNMPアクセスは信頼できるネットワークデバイスからだけ許可する必要があります。設定オプションについては、「簡易ネットワーク管理プロトコルの保護」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. 標準のセキュリティ構成を使用して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。

Cisco IOSおよびIOS XEソフトウェアのOID

```
snmp-server view SNMP_DOS ipAddressPrefixEntry.5 excluded
snmp-server view SNMP_DOS ipDefaultRouterEntry.4 excluded
snmp-server view SNMP_DOS tcp.19.1.7 excluded
snmp-server view SNMP_DOS tcp.20.1.4 excluded
snmp-server view SNMP_DOS udp.7.1.8 excluded
snmp-server view SNMP_DOS inetCidrRouteEntry.7 excluded
snmp-server view SNMP_DOS ospfv3AreaAggregateEntry.6 excluded
snmp-server view SNMP_DOS lispMappingDatabaseLocatorRlocPriority excluded
snmp-server view SNMP_DOS mplsVpnInterfaceConfEntry.2 excluded
snmp-server view SNMP_DOS mplsVpnVrfRouteTargetEntry.4 excluded
snmp-server view SNMP_DOS mplsVpnVrfBgpNbrAddrEntry.2 excluded
snmp-server view SNMP_DOS nhrpCachePrefixLength excluded
snmp-server view SNMP_DOS nhrpServerCacheAuthoritative excluded
snmp-server view SNMP_DOS nlmLogEntry.2 excluded
snmp-server view SNMP_DOS nlmLogVariableEntry.2 excluded
snmp-server view SNMP_DOS mplsXCLspId excluded
snmp-server view SNMP_DOS mplsLabelStackLabel excluded
snmp-server view SNMP_DOS cpaeMIBObject.5.1.3 excluded
```

```
snmp-server view SNMP_DOS cContextMappingBridgeDomainIdentifier excluded
snmp-server view SNMP_DOS cilmCurrentImageLevel excluded
snmp-server view SNMP_DOS cilmImageLicenseImageLevel excluded
snmp-server view SNMP_DOS cewProxyClass excluded
snmp-server view SNMP_DOS cewEventTime excluded
snmp-server view SNMP_DOS cpwVcPeerMappingVcIndex excluded
snmp-server view SNMP_DOS ciiSummAddrEntry excluded
snmp-server view SNMP_DOS mplsLdpLspFecStorageType excluded
snmp-server view SNMP_DOS mplsL3VpnIfConfEntry.2 excluded
snmp-server view SNMP_DOS mplsL3VpnVrfRTEntry.4 excluded
snmp-server view SNMP_DOS mplsL3VpnVrfRteEntry.7 excluded
snmp-server view SNMP_DOS ciscoFlashChipEntry excluded
snmp-server view SNMP_DOS cbgpPeer2CapValue excluded
snmp-server view SNMP_DOS cbgpPeer2AddrFamilyName excluded
snmp-server view SNMP_DOS cbgpPeer2AcceptedPrefixes excluded
snmp-server view SNMP_DOS callHomeDestEmailAddressEntry.2 excluded
snmp-server view SNMP_DOS callHomeSwInventoryEntry.3 excluded
snmp-server view SNMP_DOS cEigrpActive excluded
snmp-server view SNMP_DOS cipUrpfVrfIfDrops excluded
snmp-server view SNMP_DOS cefPathType excluded
snmp-server view SNMP_DOS cefAdjSource excluded
snmp-server view SNMP_DOS cefFESelectionSpecial excluded
snmp-server view SNMP_DOS cvVrfListVrfIndex excluded
snmp-server view SNMP_DOS ctspIpSgtMappingEntry.5 excluded
snmp-server view SNMP_DOS ciiRedistributeAddrEntry.4 excluded
snmp-server view SNMP_DOS ciiIPRAEntry.5 excluded
snmp-server view SNMP_DOS ciiLSPTLVEntry.2 excluded
snmp-server view SNMP_DOS ccmSeverityAlertGroupEntry.1 excluded
snmp-server view SNMP_DOS ccmPeriodicAlertGroupEntry.1 excluded
snmp-server view SNMP_DOS ccmPatternAlertGroupEntry.2 excluded
snmp-server view SNMP_DOS callHomeUserDefCmdEntry.2 excluded
snmp-server view SNMP_DOS ccmEventAlertGroupEntry.1 excluded
snmp-server view SNMP_DOS cipsStaticCryptomapType excluded
snmp-server view SNMP_DOS ciscoFlashFileEntry.2 excluded
```

Cisco IOS XRソフトウェアのOID

```
snmp-server view SNMP_DOS udp.7.1.8 excluded
snmp-server view SNMP_DOS tcp.19.1.7 excluded
snmp-server view SNMP_DOS tcp.20.1.4 excluded
snmp-server view SNMP_DOS inetCidrRouteEntry.7 excluded
snmp-server view SNMP_DOS ipAddressPrefixEntry.5 excluded
snmp-server view SNMP_DOS ipDefaultRouterEntry.4 excluded
snmp-server view SNMP_DOS 1.3.6.1.2.1.191.1.12.1.6 excluded
snmp-server view SNMP_DOS 1.3.6.1.2.1.92.1.3.1.1.2 excluded
snmp-server view SNMP_DOS 1.3.6.1.2.1.92.1.3.2.1.2 excluded
snmp-server view SNMP_DOS 1.3.6.1.4.1.9.10.106.1.7.1.5 excluded
snmp-server view SNMP_DOS 1.3.6.1.4.1.9.10.106.1.8.1.5 excluded
snmp-server view SNMP_DOS 1.3.6.1.4.1.9.9.171.1.2.2.1.6 excluded
snmp-server view SNMP_DOS 1.3.6.1.4.1.9.9.171.1.2.4.1.7 excluded
snmp-server view SNMP_DOS 1.3.6.1.4.1.9.9.187.1.1.1.1.7 excluded
snmp-server view SNMP_DOS 1.3.6.1.4.1.9.9.187.1.2.6.1.3 excluded
snmp-server view SNMP_DOS 1.3.6.1.4.1.9.9.187.1.2.7.1.3 excluded
snmp-server view SNMP_DOS 1.3.6.1.4.1.9.9.187.1.2.8.1.1 excluded
snmp-server view SNMP_DOS 1.3.6.1.2.1.10.166.4.1.3.10.1.4 excluded
snmp-server view SNMP_DOS 1.3.6.1.4.1.9.10.62.1.2.3.3.1.2 excluded
```

SNMP v1またはv2cの場合は、この設定をすべての設定済みコミュニティストリングに適用します。次のコマンドを使用します。

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

SNMP v3の場合、次のコマンドを使用して、設定されているすべてのSNMPユーザにこれを適用します。

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

これら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、このアドバイザリに記載された脆弱性に対処する無償のソフトウェアアップデートをリリースする予定です。通常のソフトウェアアップデートが含まれるサービス契約をお持ちのお客様は、通常のアップデートチャネルからセキュリティ修正を取得する必要があります。

お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。そのようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。
https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限ります。通常、これは以前購入したソフトウェアのメンテナンス アップグレードです。無償のセキュリティ ソフトウェア アップデートによって、お客様に新しいソフトウェア ライセンス、追加ソフトウェア フィーチャ セット、またはメジャー リビジョン アップグレードに対する権限が付与されることはありません。

Cisco.com の シスコサポート & ダウンロードページには、ライセンスとダウンロードに関する情報が記載されています。このページには、[マイデバイス（My Devices）] ツールを使用するお客

様のカスタマーデバイスサポート範囲も表示できます。

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。

サービス契約をご利用でないお客様

シスコから直接購入したがシスコのサービス契約をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを購入先から入手できない場合は、Cisco TAC（https://www.cisco.com/c/ja_jp/support/web/tsd-cisco-worldwide-contacts.html）に連絡してアップグレードを入手してください。

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

修正済みリリース

次の表では、左の列にシスコソフトウェアのリリースを記載しています。右の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこれらの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

IOS および IOS XE ソフトウェア

Cisco IOS ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
15.2E	15.2(7)E12（2025年3月）
15.5SY	15.5(1)SY15（2025年3月）
1590万	15.9(3)M11（2025年2月）

Cisco IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
3.11E	3.11.12E（2025年3月）
16.12	16.12.13（2025年3月）
17.9	17.9.7（2025年3月）
17.12	17.12.5（2025年2月）

Cisco IOS XE ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
17.15	17.15.3（2025年3月）

最新かつ正確な情報については、Cisco IOSおよびIOS XEソフトウェアチェッカーを使用してください。

IOSおよびIOS XEソフトウェアチェッカー

お客様がCisco IOSソフトウェアおよびIOS XEソフトウェアの脆弱性による侵害を受ける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ページにアクセスし、指示に従ってください。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、重大または高セキュリティ影響評価(SIR)のアドバイザリのみ、またはすべてのアドバイザリを選択できます。
2. リリース番号を入力します(例：15.9(3)M2、17.3.3)。
3. 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

IOS XR ソフトウェア

Cisco IOS XR ソフトウェア リリース	First Fixed Release（修正された最初のリリース）
24.2 以前	24.2.21
24.3	修正済みリリースに移行。
24.4	24.4.2
25.2	25.2.1

最新リリース情報については、CSCwn08493を参照してください。

Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正されたリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、このアドバイザリに記載されている脆弱性のいかなる悪用も認識していません。

出典

シスコは、これらの脆弱性を報告していただいたleg00m氏とTrend Micro Zero Day Initiativeの協力に感謝いたします。

URL

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

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2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。