Cisco IOSおよびIOS XEソフトウェアのSNMP拡張名前付きアクセスコントロールリスト(NACL)バイパスの脆弱性

Medium

アドバイザリーID : cisco-sa-snmp-uwBXfqww
初公開日 : 2024-04-17 16:00
バージョン 1.0 : Final
CVSSスコア : 5.3
回避策 : Yes
Cisco バグ ID : CSCwe24431

CVE-2024-20373

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)IPv4アクセスコントロールリスト(ACL)機能の実装における脆弱性により、SNMPトラフィックを拒否するように設定されている場合でも、認証されていないリモートの攻撃者が該当デバイスのSNMPポーリングを実行できる可能性があります。

この脆弱性は、Cisco IOSソフトウェアおよびCisco IOS XEソフトウェアがSNMPの拡張IPv4 ACLをサポートしていないにもかかわらず、管理者が警告メッセージを表示することなく、SNMPサーバ設定に割り当てられた名前付き拡張IPv4 ACLを設定できることを理由としています。これにより、SNMPリスニングプロセスにACLが適用されない可能性があります。攻撃者は、該当デバイスのSNMPポーリングを実行することで、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、攻撃者は拒否する必要のあるSNMP操作を実行できる可能性があります。攻撃者はSNMP ACL設定を制御できず、有効なSNMPバージョン2c(SNMPv2c)コミュニティストリングまたはSNMPバージョン3(SNMPv3)ユーザクレデンシャルを必要とします。

IPv6 ACL設定のSNMPは影響を受けません。

詳細については、このアドバイザリの「詳細情報」のセクションを参照してください。

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-

uwBXfqww

該当製品

脆弱性のある製品

公開時点で、拡張名前付きACLが適用された状態でSNMP機能が有効になっている場合、この脆弱性はCisco IOSソフトウェアおよびIOS XEソフトウェアに影響を与えました。

公開時点で脆弱性が確認されている Cisco ソフトウェアの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

ステップ 1：SNMPv2cに名前付きACLが接続されているかどうかの確認

ACLが接続されてSNMPv2cが設定されているかどうかを確認するには、show running-config | | include snmp-server コマンドを使用します。コマンドの出力が返された場合は、次の設定項目のいずれかを確認します。また、ACLが添付されている場合は、ACLの名前をメモします。次の出力例は、ExtendedIPv4ACLという名前付きACLがアタッチされていることを示しています。

<#root>

snmp-server community public ro

ExtendedIPv4ACL

snmp-server tftp-server-list

ExtendedIPv4ACL

snmp-server file-transfer access-group

ExtendedIPv4ACL

snmp-server drop report access

ExtendedIPv4ACL

ステップ 2：SNMPv3に名前付きACLが接続されているかどうかを確認する

ACLが添付された状態でSNMPv3グループが設定されているかどうかを確認するには、show running-config | | include snmp-server group コマンドを使用します。コマンドによって出力が返される場合は、キーワードaccessの後にACL名が続いているかどうかを確認します。ACLが添付されている場合は、ACLの名前をメモします。次の出力例は、ExtendedIPv4ACLという名前付きACLを示しています。

<#root>

```
snmp-server group SNMPV3_READ v3 priv read ALL write NONE notify NONE access
```

ExtendedIPv4ACL

SNMPv3では、ACLをSNMPv3ユーザに割り当てることもできます。ACLがSNMPv3ユーザに割り当てられているかどうかを確認するには、show snmp userコマンドを使用します。ユーザにACLが割り当てられている場合は、出力に表示されます。ACLが添付されている場合は、ACLの名前をメモします。次の出力例は、ExtendedIPv4ACLという名前付きACLが添付されていることを示しています。

<#root>

Router#

show snmp user

```
User name: spirit
Engine ID: 000000000000000000000000
storage-type: nonvolatile     active    access-list:
```

ExtendedIPv4ACL

```
Authentication Protocol: MD5
Privacy Protocol: DES
Group-name: SNMPV3_READ
Router#
```

ステップ 3：名前付きACLが拡張ACLであるかどうかを確認する

名前付きIPv4拡張ACLの形式は、ip access-list extended <word>です。前の2つの手順で文書化された各ACL名を使用して、show running-config | include <access-list name>コマンドを使用します。出力に、ip access-list extendedで始まる行が含まれている場合、名前付き拡張ACLがSNMP設定に接続されています。次の出力例は、ExtendedIPv4ACLという名前付きACLをチェックする方法を示しています。

<#root>

Router#

show running-config | include ExtendedIPv4ACL

```
ip access-list extended ExtendedIPv4ACL
snmp-server group SNMPV3_READ v3 priv read ALL write NONE notify NONE access ExtendedIPv4ACL
snmp-server community public RO ExtendedIPv4ACL
Router#
```

ステップ1と2で説明した各ACLについて、ステップ3を繰り返します。SNMPサーバ機能に接続されている名前付き拡張ACLが設定されている場合は、このアドバイザリの「回避策」セクションで説明されている回避策を適用します。

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記載されている製品のみが、この脆弱性の影響を受けることが分かっています。

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
- Meraki 製品
- NX-OS ソフトウェア

詳細

このセクションの情報は、SNMPがIPv4 ACLのみで設定されている場合に適用されます。SNMPに適用されたIPv6 ACL設定は影響を受けません。

SNMP設定では、標準番号付きまたは名前付きIPv4 ACLだけが許可されます。

標準ACLは、番号付きまたは名前付きのいずれかです。番号付き標準ACLには、1 ~ 99および1300 ~ 1999の番号が付けられます。標準名前付きACLは、ip access-list standard <name>コンフィギュレーションコマンドで定義され、送信元IPv4アドレスのみに基づいてパケットを許可または拒否します。

拡張ACLは、番号付きまたは名前付きにできます。番号付き拡張ACLには、100 ~ 199および2000 ~ 2699の番号が付けられます。拡張名前付きACLは、ip access-list extended <name>コンフィギュレーションコマンドで定義され、送信元と宛先のIPv4アドレス、プロトコルタイプ、送信元と宛先のTCPまたはUDPポートなどに基づいてパケットを許可または拒否します。

この脆弱性は、次の2つの形で現れます。

シナリオ 1

デバイスステータス：影響を受けるCisco IOSまたはIOS XEソフトウェアリリースを実行しており、SNMPに対する名前付き拡張ACLが設定されている

脆弱性の表示：管理者が拡張番号付きACLまたは拡張拡張番号付きACLのいずれかを追加しようとすると、パーサーがコマンドを拒否します。ただし、この脆弱性が原因で、管理者が名前付き拡張ACLを接続しようとすると、受け入れられ、設定に表示されますが、SNMPパケットの処理時には処理されません。

シナリオ 2

デバイスステータス：SNMPに対する拡張名前付きACLを使用して設定された、該当リリースのCisco IOSソフトウェアまたはIOS XEソフトウェアからのアップグレードまたはダウングレード

脆弱性の表示：管理者が名前付き拡張ACLを接続した場合、そのACLは受け入れられ、設定に表示されます。修正済みリリースへのアップグレードまたは影響を受けないリリースへのダウングレードを行うと、リブート時に拡張名ACLを持つSNMPコマンドが設定から削除されます。SNMPv3ユーザの場合、ACLは削除され、show snmp userコマンドの出力に表示されません。

両方のシナリオ：

- SNMPv2c以前のバージョンを使用して情報を取得するには、攻撃者が該当システムの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を通じて情報を取得するには、攻撃者は影響を受けるシステムのユーザクレデンシャルを持っている必要があります。

回避策

この脆弱性に対処する回避策はありません。

SNMPに対する拡張IPv4 ACLはサポートされていません。標準の番号付きおよび名前付きIPv4 ACLのみがサポートされます。

回避策は、SNMP設定に適用されているすべての拡張名前付きACLを標準名前付きACLに変更することです。

注：この脆弱性に対する修正が含まれているCisco IOSおよびIOS XEソフトウェアのリリースでは、拡張名前付きACLを適用できません。この回避策は、アップグレードの前に適用する必要があります。

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アップグレード ソリューション一式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。

修正済みリリース

注：このアドバイザリの「回避策」セクションで推奨されている変更を実装することをお勧めします。この脆弱性に対する修正を含むCisco IOSおよびIOS XEソフトウェアのリリースでは、SNMP機能に対して拡張名前付きACLを適用できません。

Cisco IOS および IOS XE ソフトウェア

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（15.9(3)M2、17.3.3 など）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 | オン

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 TAC 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-uwBXfqww

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	2024年4月17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。