Cisco IOS および Cisco IOS XE ソフトウェアの Simple Network Management Protocol におけるサービス妨害（DoS）の脆弱性

High	**アドバイザリーID :** cisco-sa-snmp-dos-USxSyTk5 **初公開日 :** 2020-06-03 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 :** CSCvk71355	CVE-2020-3235

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 Catalyst 4500 シリーズ スイッチ上の 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）サブシステムにおける脆弱性により、認証されたリモートの攻撃者がサービス妨害（DoS）状態を引き起こす可能性があります。

この脆弱性は、ソフトウェアが特定の SNMP オブジェクト ID を処理するときの入力検証が不十分であることに起因します。細工された SNMP パケットが該当デバイスに送信されると、本脆弱性がエクスプロイトされる危険性があります。不正利用に成功すると、攻撃者は該当デバイス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。

注：SNMPv2c またはそれ以前のバージョンを使用してこの脆弱性をエクスプロイトするには、攻撃者は、影響を受けるシステムの SNMP 読み取り専用コミュニティ文字列を把握している必要があります。SNMPv3 を使用してこの脆弱性をエクスプロイトするには、攻撃者は、影響を受けるシステムのユーザログイン情報を把握し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ました。この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-dos-USxSyTk5

このアドバイザリは、2020 年 6 月 3 日に公開された 25 件の脆弱性に関する 23 件のシスコ セキ

ユリティ アドバイザリを含む Cisco IOS ソフトウェアおよび IOS XE ソフトウェアリリースのセキュリティ 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、以下を参照してください。Cisco Event Response: 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、2020 年 6 月）

該当製品

脆弱性のある製品

この脆弱性は、Cisco IOS または 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ていて、SNMP ポーリング用に設定され、Power on Ethernet（PoE）ラインカードモジュールがインストールされている Cisco Catalyst 4500 シリーズ スイッチに影響を及ぼします。

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。

SNMP 設定の評価

デバイスで SNMP を使用するよう設定されているかどうかを確認するには、管理者がデバイスの CLI で **show run | include snmp**コマンドを使用します。出力が返された場合、SNMP はデバイスで有効になっています。以下に、デバイスで読み取り専用と読み取り/書き込みコミュニティ ストリングの両方が設定されている場合の **show run | include snmp**コマンドを使用します。

```
Router# show run | include snmp

snmp-server community public RO
snmp-server community write RW
```

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 Cisco IOS XR ソフトウェアまたは Cisco NX-OS ソフトウェアには影響を与えないことを確認しました。

詳細

攻撃者は、IPv4またはIPv6を使用して、巧妙に細工されたSNMPパケットを該当デバイスに送信することで、この脆弱性を不正利用する可能性があります。該当システム宛てのトラフィックだ

けが不正利用に使用できます。

SNMPv2c またはそれ以前のバージョンを使用してこの脆弱性をエクスプロイトするには、攻撃者は、影響を受けるシステムの SNMP 読み取り専用コミュニティ文字列を把握している必要があります。コミュニティ ストリングとは、デバイスの SNMP データへの読み取り専用アクセスおよび読み取り/書き込みアクセスの両方を制限するパスワードです。コミュニティ ストリングには一般的なキーワードを使用せず、他のパスワードと同様に慎重に選択してください。コミュニティ文字列は一定の間隔で変更する必要があります。また、ネットワーク管理者がロールを変更したり、組織を脱退したりする場合などには、ネットワーク セキュリティ ポリシーに従って変更する必要があります。

SNMPv3 を使用してこの脆弱性をエクスプロイトするには、攻撃者は影響を受けるシステムのユーザログイン情報を把握し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。

ただし、管理者は影響を受ける MIB を無効化することでこの脆弱性を軽減できます（この場合は、*CISCO-POWER-ETHERNET-EXT-MIB*）。view エントリを作成または更新して *CISCO-POWER-ETHERNET-EXT-MIB* を無効にする場合、次の例に示すように、管理者はデバイスにログインして、CLI で **snmp-server view グローバル コンフィギュレーション コマンドを使用できます。**

snmp-server view *SNMP_VIEW_NAME***ciscoPowerEthernetExtMIB excluded**

SNMPv2 コミュニティ文字列にこの設定を適用する場合、管理者は次のコマンドを使用できます。

snmp-server community mycomm view *SNMP_VIEW_NAME***RO**

SNMPv3 コミュニティ文字列にこの設定を適用する場合、管理者は次のコマンドを使用できます。

snmp-server group v3group v3 auth read *SNMP_VIEW_NAME***write** *SNMP_VIEW_NAME*

SNMP アクセス コントロール リスト

管理者は、アクセスコントロールリスト（ACL）を使用して特定の IP アドレスからの SNMP クエリを制限することで、攻撃対象領域を削減できます。管理者には Unicast Reverse Path Forwarding（uRPF）を使用することも推奨します。

脆弱な機能ではトランスポートとして UDP が使用されるため、攻撃者は IP アドレスをスプーフィングし、信頼できる IP アドレスからの UDP ポートへの通信を許可する ACL をバイパスする可能性があります。以下の ACL の例では、192.0.2.1 のホストのみが SNMP 要求によるデバイスへのクエリを送信できるようになっています。

```
access-list 1 permit 192.0.2.1
snmp-server community example RO 1
```

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 アップデートを提供しています。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、シスコから直接、あるいはシスコ認定リセラーまたはパートナーからそのソフトウェアの有効なライセンスを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。

ソフトウェアのアップグレードを検討する際には、Cisco Security Advisories and Alerts 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は新規リリースでも継続して適切なサポートが受けられることを確認してください。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 に連絡してアップグレードを入手してください。
https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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。

Cisco IOS および IOS XE ソフトウェア

Cisco IOS ソフトウェアおよび IOS XE ソフトウェアの脆弱性に対するリスクをお客様が判断できるように、シスコでは Cisco Software Checker を提供しています。このツールにより、特定のソフトウェアリリースに影響を及ぼすシスコ セキュリティ アドバイザリ、および各アドバイザリで説明されている脆弱性が修正された最初のリリース（「First Fixed」）を特定できます。また該当する場合、すべてのアドバイザリに記載された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。

お客様は、Cisco Software Checker を使用して次の方法でアドバイザリを検索できます。

- ソフトウェアと 1 つ以上のリリースを選択します。
- 特定のリリースのリストを含む .txt ファイルをアップロードする
- show version コマンドの出力を入力する

検索を開始した後で、すべてのシスコ セキュリティ アドバイザリ、特定のアドバイザリ、または最新の公開資料に記載されているすべてのアドバイザリが含まれるように検索をカスタマイズできます。

また、次のフォームを使用して、Cisco IOSまたはIOS XEソフトウェアリリース(**15.1(4)M2**や**3.13.8Sなど)を入力して、リリースがCisco Security Advisoryの影響を受けるかどうかを確認できます。**

デフォルトでは、Cisco Software Checker の結果には、Security Impact Rating（SIR）が「重大」または「高」の脆弱性だけが含まれます。「中間」の SIR 脆弱性の結果を含めるには、Cisco.com にある Cisco Software Checker を使用して、検索をカスタマイズするときに [影響の評価（Impact Rating）] **の下にあるドロップダウンリストの [中間（Medium）]** チェックボックスをオンにします。

Cisco IOS XEソフトウェアリリースとCisco IOSソフトウェアリリースのマッピングについては、Cisco IOS IOSに応じて、Cisco IOS XE 2リリースノート、Cisco IOS XE 3Sリリースノート、またはCisco IOS XE 3SGリリースノートを参照してくださいXEソフトウェアリリース

不正利用事例と公式発表

Cisco Product Security Incident Response Team（PSIRT）では、本アドバイザリに記載されている脆弱性のエクスプロイト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 のサポート ケースの解決中に発見されました。

URL

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-dos-USxSyTk5

改訂履歴

バージョン	説明	セクション	ステータス	Date
1.0	初回公開リリース	—	最終版	2020 年 6 月 3 日

利用規約