Cisco SG350およびSG350Xシリーズマネージドスイッチの SNMPにおけるDoS脆弱性

High

アドバイザリーID : cisco-sa-sg350-snmp-dos-GEFZr2Tj
初公開日 : 2026-05-06 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 : CSCwt39853

CVE-2026-20185

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 350シリーズマネージドスイッチ(SG350)およびCisco 350Xシリーズスタッカブルマネージドスイッチ(SG350X)ファームウェアの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の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要求の応答データ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で、この脆弱性をエクスプロイト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 またはそれ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、攻撃者が該当するシステムの有効な読み取り/書き込みまたは読み取り専用 SNMP コミュニティストリングを把握している必要があります。SNMPv3 でこの脆弱性をエクスプロイトするには、攻撃者は該当するシステムの有効な SNMP ユーザーログイン情報を入手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ておらず、リリースする予定もありません。これは、該当製品がソフトウェアメンテナンスリリース終了日を過ぎているためです。Cisco Product Security Incident Response Team(PSIRT)は、サポート終了日に達するまで、これらの製品に影響を与えるセキュリティの脆弱性を引き続き評価し、開示します。

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-sg350-

snmp-dos-GEFZr2Tj

該当製品

脆弱性のある製品

この脆弱性は、Cisco SG350およびSG350Xシリーズマネージドスイッチファームウェアリリース2.5.9.54または2.5.9.55を実行し、2つ以上の60ワットPower over Ethernet(PoE)ポートが有効になっている次のシスコ製品に影響を与えます。

- SG350-28Pスイッチ
- SG350-28MPスイッチ
- SG350-52Pスイッチ
- SG350-52MPスイッチ
- SG350Xシリーズスイッチ

デバイス設定の確認

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
```

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。次の例に示すように、両方のコマンドの出力がある場合、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
```

特定のデバイスで60 WのPoEポートが有効になっているかどうかを確認するには、show running-config | include interface|power inline limit 60000コマンドを使用します。次の例に示すように、2つ以上の60ワットのポートが設定されている必要があります。

```
<#root>

Switch#

 show running-config | include interface|power inline limit 60000


interface vlan 1
interface vlan 10
interface FiveGigabitEthernet1/0/5

 power inline limit 60000

interface FiveGigabitEthernet1/0/6

 power inline limit 60000
```

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。

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、管理者がデバイスの脆弱なオブジェクトID(OID)を無効にする可能性があります。

OIDを無効または除外するには、次の手順に従います。

1. 影響を受けるOIDを除いた新しいSNMPビューを作成します。次のコマンドを使用します。

```
<#root>
```

```
snmp-server view SNMP_DOS iso included
snmp-server view SNMP_DOS rlPethPsePortTable excluded
```

2. ビューをSNMPコミュニティまたはSNMP v3グループに適用します。

- SNMP v1 または v2c の場合、設定されているすべてのコミュニティストリングにこの設定を適用します。次のコマンドを使用します。

<#root>

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

- SNMPv3の場合は、設定されているすべてのSNMPユーザにこれを適用します。次のコマンドを使用します。

<#root>

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

修正済みソフトウェア

Cisco SG350およびSG350Xは、それぞれのソフトウェアメンテナンスリリース終了日を過ぎています。このため、シスコはこのアドバイザリに記載された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おらず、リリースする予定もありません。お客様には、これらの製品のサポート終了通知を参照することをお勧めします。

Cisco 350シリーズマネージドスイッチの販売終了およびサポート終了のお知らせ

Cisco 350Xシリーズスタッカブルマネージドスイッチの販売終了およびサポート終了のお知らせ

デバイスの移行を検討する際は、[シスコセキュリティアドバイザリ（Cisco Security Advisories）] 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の有無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、お客様は、新しい製品がネットワークのニーズに十分に対応し、現在のハードウェアおよびソフトウェア構成が新しい製品によって適切にサポートされ続けることを確認する必要があります。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。

不正利用事例と公式発表

Cisco PSIRT では、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は確認しておりません。

出典

この脆弱性を報告していただいたセキュリティ研究者のRyan Moore氏に感謝いたします。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg350-snmp-dos-GEFZr2Tj

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	2026年5月6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。