Cisco Security Advisory

Cisco SG350 and SG350X Series Managed Switches SNMP Denial of Service Vulnerability

High

Advisory ID:
cisco-sa-sg350-snmp-dos-GEFZr2Tj

First Published:
2026 May 6 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwt39853

CVE-2026-20185

CWE-122

CVSS Score:
Base 7.7

Download CSAF

Email

Summary

A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco 350 Series Managed Switches (SG350) and Cisco 350X Series Stackable Managed Switches (SG350X) firmware could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to improper error handling when parsing response data for a specific SNMP request. An attacker could exploit this vulnerability by sending a specific SNMP request to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition.

This vulnerability affects SNMP versions 1, 2c, and 3. To exploit this vulnerability through SNMPv2c or earlier, the attacker must know a valid *read-write* or *read-only* SNMP community string for the affected system. To exploit this vulnerability through SNMPv3, the attacker must have valid SNMP user credentials for the affected system.

Cisco has not released and will not release software updates that address this vulnerability because the affected products are past the date for End of Software Maintenance Releases. The Cisco Product Security Incident Response Team (PSIRT) will continue to evaluate and disclose security vulnerabilities that affect these products until the Last Date of Support is reached.

There are no workarounds that address this vulnerability. However, there is a mitigation.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg350-snmp-dos-GEFZr2Tj

Affected Products

Vulnerable Products

This vulnerability affects the following Cisco products if they are running Cisco SG350 and SG350X Series Managed Switch Firmware Release 2.5.9.54 or 2.5.9.55 and have two or more 60-watt Power over Ethernet (PoE) ports enabled:

- SG350-28P Switches
- SG350-28MP Switches
- SG350-52P Switches
- SG350-52MP Switches
- SG350X Series Switches

Determine the Device Configuration

To determine whether a device has SNMPv1 or v2c enabled, use the **show running-config | include snmp-server community** CLI command. If there is output, SNMP is enabled, as shown in the following example:

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


To determine whether a device has SNMPv3 enabled, use the **show running-c** ser CLI commands. If there is output from both commands, SNMPv3 is enabled, as shown in the following example:

```
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
```

To determine whether a device has 60 Watt PoE ports enabled, use the **show running-config | include interface|power inline limit 60000**. There must be two or more 60-watt ports configured, as shown in the following example:

```
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
```

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

Workarounds

There are no workarounds that address this vulnerability. However, as a mitigation, administrators may disable the vulnerable object ID (OID) on a device.

To disable and exclude the OID, complete the following steps:

1. Create a new SNMP view excluding the affected OID. Use the following commands:

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

2. Apply the view to the SNMP community or SNMP v3 group:

- For SNMP v1 or v2c, apply this configuration to all configured community strings. Use the following command:

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

- For SNMPv3, apply this to all configured SNMP users. Use the following command:

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

Fixed Software

Cisco SG350 and SG350X are past their respective dates for End of Software Maintenance Releases. For this reason, Cisco has not released and will not release software updates to address the vulnerability that is described in this advisory. Customers are advised to refer to the end-of-life notices for these products:

End-of-Sale and End-of-Life Announcement for the Cisco 350 Series Managed Switches

End-of-Sale and End-of-Life Announcement for the Cisco 350X Series Stackable Managed Switches

When considering a device migration, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories page, to determine exposure and a complete upgr

In all cases, customers should ensure that any new product will be sufficient for their network needs and that current hardware and software configurations will continue to be supported properly by the new product. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Source

Cisco would like to thank security researcher Ryan Moore for reporting this vulnerability.

URL

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

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2026-MAY-06

Legal Disclaimer

SOFTWARE DOWNLOADS AND TECHNICAL SUPPORT

The Cisco Support and Downloads page on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool. Please note that customers may download only software that was procured from Cisco directly or through a Cisco authorized reseller or partner and for which the license is still valid.

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco Technical Assistance Center (TAC). Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

When considering software upgrades, customers are advised to regularly consult the advisories for the relevant Cisco products to determine exposure and a complete upgrade solution. In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

LEGAL DISCLAIMER DETAILS

CISCO DOES NOT MAKE ANY EXPRESS OR IMPLIED GUARANTEES OR WARRANTIES OF ANY KIND, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, CISCO DOES NOT GUARANTEE THE ACCURACY OR COMPLETENESS OF THIS INFORMATION. THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Copies or summaries of the information contained in this Security Advisory may lack important information or contain factual errors. Customers are advised to visit the Cisco Security Advisories page for the most recent version of this Security Advisory. The Cisco Product Security Incident Response Team (PSIRT) assesses only the affected and fixed release information that is documented in this advisory. See the Cisco Security Vulnerability Policy for more information.

▶ Cisco Security Vulnerability Policy

▶ Subscribe to Cisco Security Notifications

▶ Related to This Advisory