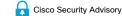
Log in

Home / Cisco Security / Security Advisories



Cisco IOS Software on Cisco Catalyst 1000 and 2960L Switches Access Control List Bypass Vulnerability



Advisory ID: cisco-sa-ipsgaclpg6qfZk

First Published:

Version 1.0:

Workarounds: Yes

Cisco Bug IDs: CSCwm03838

CVE-2025-20137

CWE-284

CVSS Score: Base 4.7

Download CSAF Email

Summary

A vulnerability in the access control list (ACL) programming of Cisco IOS Software that is running on Cisco Catalyst 1000 Switches and Cisco Catalyst 2960L Switches could allow an unauthenticated, remote attacker to bypass a configured ACL.

This vulnerability is due to the use of both an IPv4 ACL and a dynamic ACL of IP Source Guard on the same interface, which is an unsupported configuration. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device.

Note: Cisco documentation has been updated to reflect that this is an unsupported configuration. However, Cisco is publishing this advisory because the device will not prevent an administrator from configuring both features on the same interface. There are no plans to implement the ability to configure both features on the same interface on Cisco Catalyst 1000 or Catalyst 2960L Switches.

Cisco has not released software updates that address this vulnerability. There are workarounds that address this vulnerability.

This advisory is available at the following link:

 $\underline{https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipsgacl-pg6qfZk}$

Affected Products

Vulnerable Products

At the time of publication, this vulnerability affected the following Cisco products if they were running a vulnerable release of Cisco IOS Software and had both an IPv4 ACL and IP Source Guard configured on an interface:

- · Catalyst 1000 Switches
- · Catalyst 2960-L Series Switches

For information about which Cisco software releases are vulnerable, see the Fixed Software section of this advisory.

Determine the Device Configuration

To determine whether a device has an IPv4 ACL configured on the same interface that is leveraging IP Source Guard, use the show running-config CLI command. Examine the contents under each interface to see if an IPv4 access-group has been configured along with IP Source Guard, which is enabled with the ip verify source command, as shown in the following example:

```
Switch# show running-config

.
.
.
.
interface GigabitEthernet1/0/11
switchport access vlan 200
ip access-group DropACL in
ip verify source
.
.
.
Switch#
```

Note: For the IP Source Guard configuration to take effect, IP DHCP snooping must be enabled for the VLAN to which the IP Source Guard and IP access-group is applied. The following example shows DHCP enabled on VLAN 200:

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
200
DHCP snooping is operational on following VLANs:
200
.
.
.
.
output omitted
```

Products Confirmed Not Vulnerable

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

Cisco has confirmed that this vulnerability does not affect the following Cisco products:

- IOS Software that is running on platforms not listed in the <u>Vulnerable Products</u> section of this advisory
- IOS XE Software
- · IOS XR Software
- Meraki products
- NX-OS Software

∧ Details

Exploitation of this vulnerability could allow an attacker to bypass protections that are provided by an ACL that is applied on an affected device. The overall impact of exploitation is organization specific because it depends on the importance of the assets that the ACL was supposed to protect. Customers should evaluate how exploitation of this vulnerability would impact their network and proceed according to their own vulnerability-handling and remediation processes.

Either the IPv4 ACL will be active or the dynamic generated ACL for IP Source Guard will be active, but not both at the same time. The programming depends on the order of the commands, and if there are changes in IP Source Guard the ACL would be updated and reflect the IP Source Guard ACL.

Workarounds

There is a workaround that addresses this vulnerability.

Administrators should determine which ACL best suits their needs and then configure that single ACL type on the interface

While this workaround has been deployed and was proven successful in a test environment, customers should determine the applicability and effectiveness in their own environment and under their own use conditions. Customers should be aware that any workaround or mitigation that is implemented may negatively impact the functionality or performance of their network based on intrinsic customer

deployment scenarios and limitations. Customers should not deploy any workarounds or mitigations before first evaluating the applicability to their own environment and any impact to such environment.

Fixed Software

When <u>considering software upgrades</u>, customers are advised to regularly consult the advisories for Cisco products, which are available from the <u>Cisco Security Advisories page</u>, 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.

Fixed Releases

Because this vulnerability affects an unsupported feature, Cisco does not plan to release fixed software.

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

∧ Source

This vulnerability was found during the resolution of a Cisco TAC support case.

∧ URL

 $\underline{ https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipsgacl-\underline{pg6qfZk} }$

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2025-MAY-07

Legal Disclaimer

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. 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.

A standalone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy and may lack important information or contain factual errors. The information in this document is intended for end users of Cisco products.

- Cisco Security Vulnerability Policy
- Subscribe to Cisco Security Notifications
- Related to This Advisory

Your Rating:

Average Rating:

5 star 0

3 star

Quick Links		-			
About Cisco					
Contact Us					
Careers					
Connect with a partner					
Resources and Legal		-			
Feedback					
Help					
Terms & Conditions					
Privacy					
Cookies / Do not sell or share my personal data					
Accessibility					
Trademarks					
Supply Chain Transparency					
Newsroom					
Sitemap					
©2025 Cisco Systems, Inc.					

0

0

2 star

1 star

Leave additional feedback