Date: March 11, 2025

Revision	Date	Changes
1.0	March 11, 2025	Initial release

The CVE-ID tracking this issue: CVE-2024-9448
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
Common Weakness Enumeration: CWE-284 Improper Access Control
This vulnerability is being tracked by BUG 992963

Description

On affected platforms running Arista EOS with Traffic Policies configured the vulnerability will cause received untagged packets not to hit Traffic Policy rules that they are expected to hit. If the rule was to drop the packet, the packet will not be dropped and instead will be forwarded as if the rule was not in place. This could lead to packets being delivered to unexpected destinations.

Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.33.0F and below releases in the 4.33.x train
- 4.32.3M and below releases in the 4.32.x train
- 4.31.5M and below releases in the 4.31.x train
- 4.30.8M and below releases in the 4.30.x train

Affected Platforms

The following products **are** affected by this vulnerability:

- Arista EOS-based products:
  - 7050X4 Series
  - 7358X4 Series

The following product versions and platforms **are not** affected by this vulnerability:

- Arista EOS-based products:
    - 710 Series
    - 720D Series
    - 720XP/722XPM Series
    - 750X Series
    - 7010 Series
    - 7010X Series
    - 7020R Series
    - 7130 Series running EOS
    - 7150 Series
    - 7160 Series
    - 7170 Series
    - 7060X/X2/X4/X5/X6 Series
    - 7050X/7050X2/7050X3
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7800R3/R4 Series
    - 7700R4 Series
    - AWE 5000 Series
    - AWE 7200R Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2024-9448, the following condition must be met:

A Traffic Policy must be configured:

```
switch>show traffic-policy vlan
Traffic policy myPolicy
   Configured on VLANs: 42, 43
   Applied on VLANs for IPv4 traffic: 42, 43
   Applied on VLANs for IPv6 traffic: 42, 43
   Total number of rules configured: 4
      match anIpv4Rule ipv4
         Actions: Drop
      match anIpv6Rule ipv6
         Actions: Drop
      match ipv4-all-default ipv4
      match ipv6-all-default ipv6
switch>
```

If a Traffic Policy is not configured there is no exposure to this issue and the message will look something like:

```
switch>show traffic-policy vlan
switch>
```

Indicators of Compromise

This vulnerability will cause received untagged packets not to hit Traffic Policy rules that they are expected to hit. If the rule was to drop the packet will not be dropped and instead will be forwarded as if the rule was not in place.

Mitigation

There is no mitigation other than to not use the Traffic Policy feature where it would be expected to match on receipt of untagged packets.

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest

convenience. Arista recommends customers move to the latest version of each release that contains all the fixes listed below. For more information about upgrading see EOS User Manual: Upgrades and Downgrades

CVE-2024-9448 has been fixed in the following releases:

- 4.33.1F and later releases in the 4.33.x train
- 4.32.4M and later releases in the 4.32.x train
- 4.31.6M and later releases in the 4.31.x train
- 4.30.9M and later releases in the 4.30.x train

Hotfix

No hotfix is available for this issue

For More Information

If you require further assistance, or if you have any further questions regarding this security notice, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

Open a Service Request

Contact information needed to open a new service request may be found at: https://www.arista.com/en/support/customer-support