**Date: September 9, 2026**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | September 9, 2026 | Initial release |

The CVE-ID tracking this issue: CVE-2026-73461
CVSSv3.1 Base Score: 8.0 (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H)
CVSSv4.0 Base Score: 9.4
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-266: Incorrect Privilege Assignment
This vulnerability is being tracked by BUG 1602589

# Description

On affected platforms running Arista EOS, if AAA based gRPC request authorization is enabled for OpenConfig, then the gRPC requests of an authenticated user to OpenConfig may use the wrong privilege level, resulting in an authorization using the wrong AAA method list. This doesn’t affect authorization of non-gRPC requests to OpenConfig such as NETCONF.

This issue was discovered internally by Arista, and the company is not aware of any malicious exploitation of this vulnerability in customer networks.

# Vulnerability Assessment

## Platform and Software Applicability Note

To determine actual exposure, operators should first check their software versions against the "Affected Software" list below. If your software release is not listed, your deployment is not vulnerable, regardless of the hardware platform in use.

## Affected Software

### EOS Versions

- 4.36.0.1F and below releases in the 4.36.x train
- 4.35.5M and below releases in the 4.35.x train
- 4.34.7M and below releases in the 4.34.x train
- 4.33.8M and below releases in the 4.33.x train
- 4.32.11M and below releases in the 4.32.x train
- All releases in train 4.29.x, 4.30.x and 4.31.x trains

## Affected Platforms

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

- Arista EOS-based products:
  - 710 Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series
  - 7010TX Series
  - 7020R/R4 Series
  - 7130 Series running EOS
  - 7170 Series
  - 7050X3/X4 Series
  - 7060X/X2/X4/X5/X6 Series
  - 7260X/X3 Series
  - 7280R/R2/R3/R4 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Serie
  - 7500R/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

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

- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision Appliance Software
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- DANZ Monitoring Fabric (DMF) - Controller Appliance
- DANZ Monitoring Fabric (DMF) - Analytics Node Appliance
- DANZ Monitoring Fabric (DMF) - Recorder Node Appliance
- DANZ Monitoring Fabric (DMF) - Service Node Appliance
- Arista Multi Cloud Director (formerly Big Switch MCD)
- 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)
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

### Required Configuration for Exploitation

In order to be vulnerable to CVE-2026-73461, mutual TLS must be configured on an OpenConfig gRPC transport that has gRPC authorization enabled. The following show commands indicate the required config.

1. An OpenConfig gRPC transport configured with an SSL profile and request authorization:

```
switch#show man api gnmi
Transport: default
Enabled: yes
Server: running on port 6030, in default VRF
SSL profile: oc
QoS DSCP: none
Connection limit: 100
Authorization required: yes
Accounting requests: no
Notification timestamp: last change time
Listen addresses: ::
Authentication username priority: x509-spiffe, metadata, x509-common-name
Config-commands AAA accounting: enabled
Config-commands AAA authorization: enabled
```

2. The SSL profile in point 1 must be configured with a trust certificate:

```
switch#show man security ssl profile oc detail | grep Trusted -A 1
Trusted certificates:
        - shared_ca.crt
```

## Indicators of Compromise

First, enable AAA command accounting for gRPC requests to OpenConfig with the following commands:

```
switch(config)#aaa accounting commands all default start-stop logging
switch(config)#management api gnmi
switch(config-mgmt-api-gnmi)#transport grpc default
switch(config-gnmi-transport-default)#accounting requests
```

Then, an indicator of compromise would be that in the accounting logs, a gRPC request from a user X is authorized at privilege level 0 but X's privilege in the local database / TACACS+ / RADIUS is not 0. In the following example, local user bob's privilege level 9 is replaced with privilege level 0 in the gNMI GET request.

```
switch#show users accounts
user: bob
       role: none
       privilege level: 9
switch#show logging | grep ACCOUNTING
Jun 11 02:28:35 cob307 Aaa: %ACCOUNTIN
G-6-CMD: bob
 gRPC 127.0.0.1 stop task_id=33 start_time=1781170115.0134168 timezone=PDT service=sh
ell priv-lvl=0
 cmd=OpenConfig.Get addr=127.0.0.1:38120 rpc=/gnmi.gNMI/Get request=]} <cr>
```

## Mitigation

A workaround is to ensure that the authorization method list for privilege level 0 does not include 'none', which may be included alongside other methods (i.e. include some authorization method list for privilege level 0). For example, if authorization is configured using local users and TACACS+, privilege level 0 authorization can be defined as follows:

```
switch(config)#aaa authorization exec default local group tacacs+
switch(config)#aaa authorization commands 0 default local group tacacs+
```

## 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-2026-73461 has been fixed in the following releases:

- 4.36.1F and later releases in the 4.36.x train
- 4.35.6M and later releases in the 4.35.x train
- 4.34.8M and later releases in the 4.34.x train
- 4.33.9M and later releases in the 4.33.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