Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release
1.1	September 22, 2026	CSAF JSON file added

The CVE-ID tracking this issue: CVE-2026-19640
CVSSv3.1 Base Score: 4.2 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N)
CVSSv4.0 Base Score: 2.3
(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-863: Incorrect Authorization
This vulnerability is being tracked by BUG 1602635, BUG 1602639

Description

On affected platforms running Arista EOS, an authenticated user with access to the gNMI(gRPC Network Management Interface) may receive incorrect authorization results, potentially allowing access beyond their currently assigned permissions.

This issue was discovered internally by Arista and the company is not aware of any malicious uses of this issue 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
- All releases in between the 4.24.x and 4.32.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 Series
  - 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:

- WI-FI 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-2026-19640, OpenConfig with authorized requests must be configured:

```
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
```

Indicators of Compromise

No reliable indicators of compromise exist.

Mitigation

The vulnerability can be mitigated by performing both of the following actions.

1. Kill gNMI subscriptions after AAA authorization policy changes. Run the following command to kill gNMI subscriptions to OpenConfig/Octa on port 6030. If a different port than the default of 6030 is being used for OpenConfig/Octa, adjust accordingly to that port:

```
switch#bash ss -tnp dport = 6030
```

```
| grep -o 'pid=[0-9]*' | cut -d= -f2 | xargs sudo kill
```

Note: the port that OpenConfig/Octa is running the gNMI transport on is available in the output of the **show man api gnmi** CLI command (see above under the Server: field)

2. Use username and password based authentication (as opposed to mTLS) for gNMI requests to OpenConfig/Octa. The following command is an example using Arista's gNMI client:

```
gnmi -username bob -password myPass123 -addr 127.0.0.1 subscribe /system/state
```

For a transport running mTLS, mTLS can be disabled for this transport by any of the configurations described below:

1. Configure the SSL profile to use TLS instead of mTLS. This can be done by removing the trusted certificates from the SSL profile, using the "**no trust certificate <name>**" CLI command within the SSL profile.

   For example, if an SSL profile has configuration like:

```
management security
   ssl profile XXY
      certificate x.crt key x.key
      trust certificate A.crt
      trust certificate B.crt
```

   Then this profile can be changed from mTLS to TLS by removing each of the trusted certificates:

```
switch#configure
switch(config)#management security
switch(config-mgmt-security)#ssl profile XXY
switch(config-mgmt-sec-ssl-profile-XXY)#no trust certificate A.crt
switch(config-mgmt-sec-ssl-profile-XXY)#no trust certificate B.crt
```

   Note that if other transports or servers on the system have configured to use this

SSL profile, then the above configuration will also cause them to transition from mTLS to TLs.

2. Configure the OpenConfig/Octa transport to use an insecure server instead of mTLS, by removing the SSL profile config from the "**transport grpc <name>**" mode. This can be done by running the "**no ssl profile**" command as shown:

```
switch#configure
switch(config)#management api gnmi
switch(config-mgmt-api-gnmi)#transport grpc default
switch(config-gnmi-transport-default)#no ssl profile
```

When this is done, the show command will display that no SSL profile is configured:

```
switch#show man api gnmi
Transport: default
Enabled: yes
Server: running on port 6030, in default VRF
SSL profile: none
QoS DSCP: none
Connection limit: 100
Authorization required: no
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
```

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-2026-19640 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