Date: February 25, 2025

Revision	Date	Changes
1.0	February 25, 2025	Initial release

The CVE-ID tracking this issue: CVE-2025-1259
CVSSv3.1 Base Score: 7.7 (CVSS:3.1 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N)
Common Weakness Enumeration: CWE-284: Improper Access Control
This vulnerability is being tracked by BUG 1015822

The CVE-ID tracking this issue: CVE-2025-1260
CVSSv3.1 Base Score: 9.1 (CVSS:3.1 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)
Common Weakness Enumeration: CWE-284: Improper Access Control
This vulnerability is being tracked by BUG 1015821

Description

For both CVE-2025-1259 and CVE-2025-1260, on affected platforms running Arista EOS with OpenConfig configured, a gNOI request can be run when it should have been rejected.

CVE-2025-1259 can result in users retrieving data that should not have been available.

CVE-2025-1260 can result in unexpected configuration/operations being applied to the switch.

These issues were discovered internally, and Arista is unaware of any malicious uses of these issues in customer networks. These are similar types of authorization issues and are being released together due to their similarity.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.33.1 and below releases in the 4.33.x train
- 4.32.3 and below releases in the 4.32.x train
- 4.31.5 and below releases in the 4.31.x train
- 4.30.8 and below releases in the 4.30.x train
- 4.29.9 and below releases in the 4.29.x train
- 4.28.12 and below releases in the 4.28.x train

Affected Platforms

The following products **are** 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
    - 7050X/X2/X3/X4 Series
    - 7060X/X2/X4/X5/X6 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7800R3/R4 Series
    - 7700R4 Series
    - AWE 5000 and AWE 7200R Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab

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

- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- 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)
- Arista Wireless Access Points

Required Configuration for Exploitation

To be vulnerable to CVE-2025-1259 and CVE-2025-1260 the only condition is that OpenConfig must be enabled with a gNOI server.

```
switch(config-gnmi-transport-default)#show management api gnmi
Transport: default
Enabled: yes
Server: running on port 6030, in default VRF
SSL profile: none
QoS DSCP: none
Authorization required: no
Accounting requests: no
Notification timestamp: last change time
Listen addresses: ::
Authentication username priority: x509-spiffe, metadata, x509-common-
name
```

If OpenConfig is not configured or OpenConfig is configured with no gNOI server, then there is no exposure to this issue and the message will look like.

```
switch(config)#show management api gnmi
Enabled: no transports enabled
```

Indicators of Compromise

No indicators of compromise exist.

Mitigation

EOS 4.31.0F and later releases

For releases with gNSI Authz (EOS 4.31.0F and later releases), the gNOI RPC’s can be blocked using gNSI Authz.

First enable gNSI Authz service by adding the following config:

```
switch(config)#management api gnsi
switch(config-mgmt-api-gnsi)#service authz
(config-mgmt-api-gnsi)#transport gnmi [NAME]
```

Where [NAME] is the name of the running gNMI transport which gNSI will run on. Adding this config will cause the named gNMI transport to reload.

Next update the authz policy to block access to the TransferToRemote RPC. This can be done directly on the system by updating the Authz policy file and waiting at least 10 seconds for OpenConfig to reload the changes. Note this will replace any existing authz policies located at /persist/sys/gnsi/authz/policy.json

For CVE-2025-1259 the following CLI command (highlighted in yellow following the switch prompt) can be run which will disable all gNOI Get RPC's.

```
switch#
bash timeout 100 echo "],\"deny_rules\":[}]}" | sudo tee /persist/sys/
gnsi/authz/policy.json && sleep 11
```

For CVE-2025-1260 the following CLI command (highlighted in yellow following the switch prompt) can be run which will disable all gNOI Set RPC's.

```
switch#
bash timeout 100 echo "],\"deny_rules\":[}]}" | sudo tee /persist/sys/
gnsi/authz/policy.json && sleep 11
```

To resolve both CVE's the following CLI command can be ran which will disable all gNOI RPC's.

```
switch#
bash timeout 100 echo "],\"deny_rules\":[}]}" | sudo tee /persist/sys/
gnsi/authz/policy.json && sleep 11
```

All releases

For CVE-2025-1260 the workaround is to disable gNOI Set requests. This can be done by applying per RPC authorization and ensuring no user can run the OpenConfig.Set command.

For CVE-2025-1259 the workaround is to disable gNOI Get requests. This can be done by applying per RPC authorization and ensuring no user can run the OpenConfig.Get command.

Note these commands will also disable read/write gNMI RPC's respectively.

```
switch(config-gnmi-transport-default)#show management api gnmi
   transport grpc default
      authorization requests
```

Alternatively for both, the OpenConfig agent can be disabled.

```
switch(config-gnmi-transport-default)#no management api gnmi
```

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-2025-1259 and CVE-2025-1260 are fixed in the following releases:

- 4.33.2 and later releases in the 4.33.x train
- 4.32.4 and later releases in the 4.32.x train
- 4.31.6 and later releases in the 4.31.x train

- 4.30.9 and later releases in the 4.30.x train
- 4.29.10 and later releases in the 4.29.x train
- 4.28.13 and later releases in the 4.28.x train

Hotfix

The following hotfix can be applied to remediate CVE-2025-1259 and CVE-2025-1260. The hotfix only applies to the releases listed below and no other releases.

Note: Installing/uninstalling the SWIX will cause the OpenConfig/Octa process to restart. Services may be unavailable for up to one minute.

EOS Versions 4.33.1

- **32 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_32_4.33.1_Hotfix.swix

```
SWIX hash:(SHA512)
990f21088058ab2cc80589c4dcfc43fcb89087d0f9d0c71385e87ce08b4a6b718
0eeb3f98009b2703a9317d0f32d56c840d712236b572c4d181da03ee72936a6
```

- **64 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_64_4.33.1_Hotfix.swix

```
SWIX hash:(SHA512)
c76c94a783a8b130d5d9ea9c4e120d3ccadafac8257d381f7adfe37ad1c7d2ae6
757f4719e04867bd51b7d17d916aefded05631fa892295039b73b952a8d3ccb
```

EOS Versions 4.32.3

- **32 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_32_4.32.3_Hotfix.swix

```
SWIX hash:(SHA512)
0d57eeb0270ad376c2daab92730dabd905357e5f352c61d56a98494c902b991f7
8fc92636518a6f435e655840030236d3a35dced07b7bf1c9e1f8be85c5700ec
```

- **64 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_64_4.32.3_Hotfix.swix

```
SWIX hash:(SHA512)
9d6e986845baf787b56442f4f6d542b2b196c0e5f3f50a31dcf3e07487b2f097e
0e9aa87055dad4c7ce2f72eaf8923e074c3d760f5c00ac1e1bb9dbe35f1993c
```

EOS Versions 4.31.5

- **32 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_32_4.31.5_Hotfix.swix

```
SWIX hash:(SHA512)
37da167e99f13eb6c3dae291ef65f13a28be9d448c46cf048e27b0fd189e4254d
e7eea9fce63a2bf03353c9a653894e8543d9f21cb26c5883387acc3bf965bb5
```

- **64 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_64_4.31.5_Hotfix.swix

```
SWIX hash:(SHA512)
ffee07dc7ef0dc549471078755e2b345b3e27bcc907c9a515ad92066f551766ab
05c4ffe4666fd19e3ee377ca0fa78c0ccb637d053ba3647d9c2bb071706c379
```

EOS Versions 4.30.8

- **32 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_32_4.30.8_Hotfix.swix

```
SWIX hash:(SHA512)
3407b0d76f35cbd62561f16f064c10d8df535822223f62cd8f5b3b7a747945d39
dd055c6a5649e9557d48b8f8e26f0dbffb323a01fb799b91891213832db61f8
```

- **64 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_64_4.30.8_Hotfix.swix

```
SWIX hash:(SHA512)
bf9f4eb18072bbe8cfb73884bd0c06fab66f94cec37cb9dd648e2467b3b461617
6a47287838d58477bc4ffd65d06914536e672e0e36e4e2b74abf4260e491769
```

EOS Versions 4.29.9

- **32 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_32_4.29.9_Hotfix.swix

```
SWIX hash:(SHA512)
Be73c7fa2f684ab8fb9b7d081cba477e0e0725a5a5824f787d9b17602b268e8fe
84f46382f54d125b2bd374aaef906cb541c16e7f27cccc8b3f8fba12dc10d16
```

- **64 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_64_4.29.9_Hotfix.swix

```
SWIX hash:(SHA512)
88f8681c918c28d6ecf854f21f8a6c523faa98365d9c0cb82572a818e6bfb81e6
5e47e452a86c1d39422865c7555fd2b9c9ef533b29ae1d4e1b05ec845b02727
```

EOS Versions 4.28.12

- **32 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_32_4.28.12_Hotfix.swix

```
SWIX hash:(SHA512)
91c1ade0e6d33365420df6a8ec57d5d63c75e76e180910d63d9efa52104fffdc4
eeaa1bcb4db0fb9a7d06788fb9dc82b7b46f64fc04967defefb3b634a1dca47
```

- **64 bit**
- Version: 1.0
- URL: https://www.arista.com/en/support/advisories-notices/sa-download/?sa111-SecurityAdvisory111_CVE-2025-1259_CVE-2025-1260_64_4.28.12_Hotfix.swix

```
SWIX hash:(SHA512)
65c37c7f0c2535e5b90a426209643c2e445b8a9c0eb77772b2231784c1562f39c
6cc4378aa515d1174ef3d5f6cf0034477e0b538da4f70b02a945dbc5a1fafcb
```

For instructions on installation and verification of the hotfix patch, refer to the “managing eos extensions” section in the EOS User Manual. Ensure that the patch is made persistent across reboots by running the command ‘**copy installed-extensions boot-extensions**’.

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