Date: July 25th, 2024

Revision	Date	Changes
1.0	July 2, 2024	Initial release
1.1	July 8, 2024	Update to Required Configuration for Exploitation
1.2	July 25, 2024	Update the Hotfix applicable releases

The CVE-ID tracking this issue: CVE-2024-27892
CVSSv3.1 Base Score: 9.6 (CVSS:3.1AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H)
Common Weakness Enumeration: CWE-306 Missing Authentication for Critical Function
This vulnerability is being tracked by BUG 912475

The CVE-ID tracking this issue: CVE-2024-27890
CVSSv3.1 Base Score: 9.6 (CVSS:3.1AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H)
Common Weakness Enumeration: CWE-306 Missing Authentication for Critical Function
This vulnerability is being tracked by BUG 747512

Description

For both CVE-2024-27892 and CVE-2024-27890, affected platforms running Arista EOS with OpenConfig configured, a gNMI Set request can be run when it should have been rejected. This can result in unexpected configuration being applied to the switch. These issues are similar types of authorization issues and are being released together due to their similarity.

This issue was discovered internally and Arista is not aware of any malicious uses of this issue in customer networks

Vulnerability Assessment

Affected Software

The following EOS versions **are** affected for CVE-2024-27890

EOS Versions

- 4.29.7M and below releases in the 4.29.x train
- 4.28.10M and below releases in the 4.28.x train
- 4.27.8M and below releases in the 4.27.x train

- 4.26.9M and below releases in the 4.26.x train
- 4.25.10M and below releases in the 4.25.x train
- 4.24.11M and below releases in the 4.24.x train

The following EOS versions **are** affected for CVE-2024-27892

EOS Versions

- 4.31.2F and below releases in the 4.31.x train
- 4.30.5M and below releases in the 4.30.x train
- 4.29.7M and below releases in the 4.29.x train
- 4.28.10M and below releases in the 4.28.x train
- 4.27.8M and below releases in the 4.27.x train
- 4.26.9M and below releases in the 4.26.x train
- 4.25.10M and below releases in the 4.25.x train
- 4.24.11M and below releases in the 4.24.x train

Affected Platforms

The following products **are** affected by both vulnerabilities:

- 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 Series
- CloudEOS
- cEOS-lab
- vEOS-lab
- AWE 5000 Series

The following product versions and platforms **are not** affected by both vulnerabilities:

- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi 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)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2024-27892, the only condition is that OpenConfig must be enabled with an SSL profile.

```
switch(config-gnmi-transport-default)#show management api gnmi
Transport: default
Enabled: yes
Server: running on port 6030, in default VRF
SSL profile: profile-name
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
```

In order to be vulnerable to CVE-2024-27890, the only condition is that OpenConfig must be enabled:

```
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 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

For CVE-2024-27892 the workaround is to disable gNMI Set requests. This can be done by applying per RPC authorization and ensuring no user is authorized to run the OpenConfig.Set command.

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

```
   transport grpc default
      authorization requests
```

Alternative for CVE-2024-27892 TLS can be disabled.

```
switch(config-gnmi-transport-default)#no ssl profile
```

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-2024-27892 has been fixed in the following releases:

- 4.31.3M and later releases in the 4.31.x train
- 4.30.6M and later release in the 4.30.x train
- 4.29.8M and later releases in the 4.29.x train
- 4.28.11M and later releases in the 4.28.x train

CVE-2024-27890 has been fixed in the following releases:

- 4.30.0M and onwards
- 4.29.8M and later releases in the 4.29.x train
- 4.28.11M and later releases in the 4.28.x train

To fix both issues please upgrade to either 4.30.6, 4.31.3, or later releases.

Hotfix

The following hotfix can be applied to remediate CVE-2024-27890 and CVE-2024-27892. 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 4.30.5

32 bit
Version: 1.0
URL:
https://www.arista.com/support/advisories-notices/sa-download/?sa99-CVE-2024-27890_CVE-2024-27892_4.30.5_32_Hotfix.swix

```
SWIX hash:(SHA512)
85ec967b17231edd542800a4a5b305de93308ba5365c858470e7ce848bbc6c357be614
f2f668b4a1d93c7afa2cb5e62ac12efda00874f6801dff35351da9ed93
```

64 bit
Version: 1.0
URL:
https://www.arista.com/support/advisories-notices/sa-download/?sa99-CVE-2024-27890_CVE-2024-27892_4.30.5_64_Hotfix.swix

```
SWIX hash:(SHA512)
263331d15057c38e2e9c4af20f9795989ec962dc159c3136f4eb2e2370859866534b44
a17ba9c2ec3249071ccfe83eb0047960693864de532de44fe36766fd70
```

EOS Versions 4.29.7

32 bit
Version: 1.0
URL:
https://www.arista.com/support/advisories-notices/sa-download/?sa99-CVE-2024-27890_CVE-2024-27892_4.29.7_32_Hotfix.swix

```
SWIX hash:(SHA512)
0317d77d621fa648aa15d607c6db1a8f648da82e14e0886aea0525e0d726ff83a0ed50
7755b733d1644797dece85203dfe6998b65108b10ba5a9b9be8f57c4f0
```

64 bit
Version: 1.0
URL:
https://www.arista.com/support/advisories-notices/sa-download/?sa99-CVE-2024-27890_CVE-2024-27892_4.29.7_64_Hotfix.swix

```
SWIX hash:(SHA512)
d6d1d806fbd80d9d3972d8bb965b82cf1241c166ce960ff2af12de084c171604331886
83fe48d5e3f24ba996e4b4262e95998683c50f80ce2f870fd3f02cbdc4
```

EOS Versions 4.28.10.1

32 bit
Version: 1.0
URL:
https://www.arista.com/support/advisories-notices/sa-download/?sa99-CVE-2024-27890_CVE-2024-27892_4.28.10.1_32_Hotfix.swix

```
SWIX hash:(SHA512)
12ec36dd68decff5d81f68504dfdba0c01697153366c6de01ac5189c0250516a01d012
8179155b21bd028cbbc1b634e8bc143244a2bed089824d4dc4b6c92449
```

64 bit
Version: 1.0
URL:

https://www.arista.com/support/advisories-notices/sa-download/?sa99-CVE-2024-27890_CVE-2024-27892_4.28.10.1_64_Hotfix.swix

```
SWIX hash:(SHA512)
2f01a806867d6ffc95bef907164b3c92058382ccda5af006f66f350575a235a6f1ed49
1974b68dc952947d7cf9897028efa2266411e380da6a646719a420ec52
```

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