Date: April 25, 2023

Revision	Date	Changes
1.0	April 25, 2023	Initial release

The CVE-ID tracking this issue: CVE-2023-24512
CVSSv3.1 Base Score: 8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Common Weakness Enumeration: CWE-284 Improper Access Control
This vulnerability is being tracked by BUG751697

Description

On affected platforms running Arista EOS, an authorized attacker with permissions to perform gNMI requests could craft a request allowing it to update arbitrary configurations in the switch. This situation occurs only when the Streaming Telemetry Agent (referred to as the TerminAttr agent) is enabled and gNMI access is configured on the agent.

Note: This gNMI over the Streaming Telemetry Agent scenario is mostly commonly used when streaming to a 3rd party system and is not used by default when streaming to CloudVision.

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

Vulnerability Assessment

Affected Software

All EOS Releases with the following Streaming Telemetry Agent Versions:

- TerminAttr 1.24.3 and earlier releases in the 1.24.X train
- TerminAttr 1.23.0
- TerminAttr 1.22.1 and earlier releases in the TerminAttr 1.22.X train
- TerminAttr 1.19.5 and earlier releases

In particular, the above Streaming Telemetry Agent version shipped with the following EOS Versions

- 4.29.1F and below releases in the 4.29.x train
- 4.28.5M 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

Affected Platforms

The following products are affected by this vulnerability:

- Arista EOS-based products:
    - 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 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

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

- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- 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)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2023-24512 the following conditions must be all be met:

A vulnerable version of the Streaming Telemetry Agent must be installed on the switch. The version can be verified with the following commands:

```
#show version detail | grep TerminAttr-core
TerminAttr-core      v1.13.3         1
```

In the above example, TerminAttr 1.13.3 is installed.

The agent must be running on the switch. This can be verified as follows on the switch:

```
switch# show daemon TerminAttr
Process: TerminAttr (running with PID 2430)
```

The Streaming Telemetry Agent must be configured to allow external connections using gRPC. This can be verified by the presence of the **-grpcaddr** option:

```
switch# daemon TerminAttr
    show active
daemon TerminAttr
   exec /usr/bin/TerminAttr -grpcaddr=... <other options...>
```

Indicators of Compromise

There are no indicators in logs and syslogs.

Mitigation

The streaming telemetry agent can be configured in gRPC read-only mode by specifying **-grpcreadonly** as part of its configuration. For instance as follows:

```
switch# daemon TerminAttr
   exec /usr/bin/TerminAttr -grpcreadonly -grpcaddr=... <other options...>
   no shutdown
```

If TerminAttr is running, it must be restarted for the configuration to take effect. This can be done as follows:

```
switch# daemon TerminAttr
   shutdown
   wait-for-warmup
   no shutdown
```

Resolution

While the steps listed above resolve the issue, the recommended long term solution 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.

There are two possible solutions:

Upgrade the Streaming Telemetry Agent

Customers can upgrade the Streaming Telemetry Agent to a fixed version, following the directions in https://arista.my.site.com/AristaCommunity/s/article/terminattr-upgrade-downgrade.

Fixes are available in the following supported release trains:

- TerminAttr 1.25.0 and later Terminattr versions
- Users of 1.24.X and 1.23.X TerminAttr releases should upgrade to TerminAttr 1.25.0 or later.
- TerminAttr 1.22.2 and later version in the TerminAttr 1.22.X train
- TerminAttr 1.19.6 and later versions in the TerminAttr 1.19.X train

Upgrade EOS

Customers can upgrade to a version of EOS which contains a fixed version of the Streaming Telemetry Agent within the EOS image, as documented in https://www.arista.com/en/um-eos/eos-upgradedowngrade-overview:

- EOS 4.29.2F and later releases, which contains TerminAttr 1.25.0 or a more recent version
- EOS 4.28.6M and later releases in the 4.28.X train, which contains TerminAttr 1.22.2 or a more recent version
- EOS 4.27.9M and later releases in the 4.27.X train, which contains TerminAttr 1.19.6 or a more recent version
- EOS 4.26.10M and later releases in the 4.26.X train, which contains TerminAttr 1.19.6 or a more recent version

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

By email: support@arista.com
By telephone: 408-547-5502 ; 866-476-0000
Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support