Date: June 23, 2026

Revision	Date	Changes
1.0	Jun 23, 2026	Initial release

Description

All of the CVEs covered in this advisory apply to affected platforms running Arista EOS with the Streaming Telemetry Agent (aka TerminAttr) enabled. This issue primarily affects customers using the Streaming Telemetry Agent to connect to CloudVision or a gNMI server.

All of these issues were discovered internally by Arista and Arista is not aware of any malicious uses of these issues in customer networks.

1) CVE-2026-11704

Unexpected data can be streamed to CloudVision.

CVSSv3.1 Base Score: 4.1 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N)
CVSSv4.0 Base Score: 6.4
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-312: Cleartext Storage of Sensitive Information

This vulnerability is being tracked by BUG1592886 and BUG1592639.

2) CVE-2026-11705

System data may be modified via a crafted set of packets if Streaming Telemetry Agent is active in a specific, non-default configuration.

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)
CVSSv4.0 Base Score: 9.0
(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-250: Execution with Unnecessary Privileges

This vulnerability is being tracked by BUG1592927.

3) CVE-2026-52895

User credentials can be seen and altered by users logged into the device.

CVSSv3.1 Base Score: 6.3 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L)
CVSSv4.0 Base Score: 4.8
(CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:L/SA:N)
Common Weakness Enumeration: CWE-276: Incorrect Default Permissions

This vulnerability is being tracked by BUG1595943.

4) CVE-2026-52896

In certain configurations Streaming Telemetry Agent may improperly validate a certificate.

CVSSv3.1 Base Score: 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
CVSSv4.0 Base Score: 8.2
(CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-295: Improper Certificate Validation

This vulnerability is being tracked by BUG1592931.

5) CVE-2026-52897

The privilege levels of users authenticated to the device may exceed intended restrictions, enabling unauthorized operations.

CVSSv3.1 Base Score: 3.8 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N)
CVSSv4.0 Base Score: 6.3
(CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-269: Improper Privilege Management

This vulnerability is being tracked by BUG1592936.

6) CVE-2026-52898

Streaming Telemetry Agent could provide unintended data when processed with a specifically designed sequence of packets.

CVSSv3.1 Base Score: 4.3 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)
CVSSv4.0 Base Score: 2.3
(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-668: Exposure of Resource to Wrong Sphere

This vulnerability is being tracked by BUG1611145.

Vulnerability Assessment

Affected Software

Streaming Telemetry Agent (TerminAttr) Versions:

- v1.44.0
- v1.43.5 and below releases in the v1.43 train

- All releases in the v1.42 train
- All releases in the v1.41 train
- v1.40.9 and below releases in the v1.40 train
- All releases in the v1.39 train
- All releases in the v1.38 train
- v1.37.10 and below releases in the v1.37 train
- All releases in the v1.36 train
- All releases in the v1.35 train
- v1.34.12 and below releases in the v1.34 train
- All releases in the v1.33 train
- All releases in the v1.32 train
- v1.31.15 and below releases in the v1.31 train
- All releases in all trains prior to v1.31

The above Streaming Telemetry Agent version shipped with the following EOS Versions:

EOS Versions

- 4.36.0F
- 4.35.5M and below releases in the 4.35 train
- 4.34.7M and below releases in the 4.34 train
- 4.33.8M and below releases in the 4.33 train
- 4.32.11M and below releases in the 4.32 train
- 4.31.10M and below releases in the 4.31 train
- All releases in all trains before 4.31

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/R4 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/R4 Series
- 7300X/X3 Series
- 7320X Series
- 7358X4 Series
- 7368X4 Series
- 7388X5 Series
- 7500E/R/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 as-a-Service
- CloudVision AGNI - Cloud service delivery
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch 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)
- 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

For all of the CVEs described in this document a prerequisite configuration is for a vulnerable version of the Streaming Telemetry Agent must be installed on the switch. The version can be verified with the following commands:

```
switch#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)
```

Some specific CVEs below also have other prerequisites listed below.

CVE-2026-11704 and CVE-2026-52897

For CVE-2026-11704 and CVE-2026-52897 the following is a prerequisite:
The Streaming Telemetry Agent must be configured to stream to CloudVision. This can be verified by the presence of the -cvaddr or the -cvopt options:

```
switch>en
switch#config
switch(config)#daemon TerminAttr
switch(config-daemon-TerminAttr)#show active
daemon TerminAttr
   exec /usr/bin/TerminAttr  -cvaddr=... <other options...>
```

CVE-2026-11705

For CVE-2026-11705 the following is a prerequisite:
The Streaming Telemetry Agent must be configured to stream as TerminAttrRW. This can be verified by the binary name in the exec as TerminAttrRW:

```
switch>en
switch#config
switch(config)#daemon TerminAttr
switch(config-daemon-TerminAttr)#show active
daemon TerminAttr
   exec /usr/bin/TerminAttrRW <options>
```

In the example above the agent is configured to stream as “TerminAttrRW”

CVE-2026-52896

For CVE-2026-52896 the following is a prerequisite:
The Streaming Telemetry Agent must be configured with grpc tunnel. This can be verified by the presence of the -grpctunnel_addr option:

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

CVE-2026-52898

For CVE-2026-52898 the following is a prerequisite:
The Streaming Telemetry Agent must be configured to stream to CloudVision and be running with the -cveapimode=queued flag.

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

Indicators of Compromise

There are no indicators of compromise for any of the CVEs listed in this document.

Mitigation

CVE-2026-11705

Avoid running Streaming Telemetry Agent (TerminAttr) with the binary name TerminAttrRW.

CVE-2026-52898

Avoid using the -cveapimode=queued flag with Streaming Telemetry Agent (TerminAttr).

Resolution

Hotfix (Streaming Telemetry Agent Upgrade Only)

The recommended resolution for all of the CVEs listed in this document is to upgrade to a remediated version of the Streaming Telemetry Agent (TerminAttr) per the table below:

EOS Version	Applicable TerminAttr Versions with the fixes
< EOS 4.27	v1.31.16 and later releases on the v1.31 train
EOS 4.27	v1.34.13 and later releases on the v1.34 train
EOS 4.28	v1.37.11 and later releases on the v1.37 train
EOS 4.29 and later	v1.40.10 and later releases on the v1.40 train, v1.43.6 and later releases on the v1.43 train, v1.44.1, or v1.45.0 and all later releases

Note: the upgrade of the streaming telemetry agent will momentarily affect communication to CloudVision during the upgrade process.

EOS Upgrade

If your hardware supports upgrading EOS and you prefer upgrading to a version of EOS that contains the fixed Streaming Telemetry Agent, all of the CVEs listed in this document will be fixed in the following EOS releases:

- 4.33.9M and later releases in the 4.33 train (not yet available at the time of this advisory)
- 4.34.8M and later releases in the 4.34 train (not yet available at the time of this advisory)
- 4.35.6M and later releases in the 4.35 train (not yet available at the time of this advisory)
- 4.36.1F and later releases

For more information about upgrading see EOS User Manual: Upgrades and Downgrades

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