Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

Description

Both CVE-2026-73456 and CVE-2026-73457 affect Arista EOS-based platforms with gRPC Network Packet Sampling Interface (gNPSI) configured. which is disabled by default.

These issues were discovered internally by Arista and the company is not aware of any malicious uses of this issue in customer networks.

CVE-2026-73456

Under certain circumstances, an unauthenticated gNPSI client can craft a malicious request to allow arbitrary code execution, granting an attacker full administrative control over the compromised switch.

CVSSv3.1 Base Score: 10 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
CVSSv4.0 Base Score: 9.2
(CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-94: Improper Control of Generation of Code ('Code Injection')
This vulnerability is being tracked by BUG 1823956

CVE-2026-73457

Under certain circumstances, the gNPSI client credentials might be logged in clear text, in local or remote accounting logs to authenticated users.

CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N)
CVSSv4.0 Base Score: 6
(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-532: Insertion of Sensitive Information into Log File
This vulnerability is being tracked by BUG 1824885

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

- 4.36.1F and below releases in the 4.36.x train
- 4.35.5M and below releases in the 4.35.x train
- releases between 4.34.2F and 4.34.7M in the 4.34.x train

Affected Platforms

The following products **are** affected by CVE-2026-73456 and CVE-2026-73457:

- 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-2026-73456, one of the following conditions must be met:
A gNPSI transport must be configured to perform TLS (server verification) and metadata authentication has to be enabled.

```
switch> show management api gnpsi
Transport: t2
Enabled: yes
Server: running on port 7001
Source: sflow
Listening VRF default: ::
SSL profile: P2, TLS configured
Authentication username priority: x509-spiffe, metadata, x509-common-name
Accounting requests: no
sFlow received datagrams: 0
sFlow dropped datagrams: 0
Active client subscriptions: 0
```

Or mTLS enabled with *x509-common-name* authentication configured.

```
switch> show management api gnpsi
```

```
Transport: t2
Enabled: yes
Server: running on port 7001
Source: sflow
Listening VRF default: ::
SSL profile: P2, mutual TLS configured
Authentication username priority: x509-spiffe, x509-common-name
Accounting requests: no
sFlow received datagrams: 0
sFlow dropped datagrams: 0
Active client subscriptions: 0
```

In order to be vulnerable to CVE-2026-73457, gNPSI must be configured with trace facility EosRpcAuth enabled explicitly:

```
switch> show trace Gnpsi | grep Auth
EosRpcAuth           enabled  0123456789.
```

Systems remain unaffected by either CVE-2026-73456 or CVE-2026-73457 if gNPSI is not enabled, which is the default configuration.

```
switch> show management api gnpsi
Enabled: no transports enabled
```

Indicators of Compromise

There are no reliable indicators of compromise for CVE-2026-73456.

In the case of CVE-2026-73457, though, a message like this can appear in the Gnpsi agent log:

```
AaaApi.authenticateAndOpenSessionExec( user='someUser', password='mySecretPassword',
service='gRPC', remoteHost='10.22.33.44', localAddr='10.77.88.99', localPort=9090, re
motePort=45231, taskIds=['12345'])
```

Mitigation

To secure the agent against both CVE-2026-73456 and CVE-2026-73457, the service must be configured to use *mutual TLS* and only *x509-spiffe* authentication must be enabled.

```
management security
   ssl profile P1
      certificate server.crt key server.key
      trust certificate ca_client.crt
      chain certificate ca_signing.crt
!
management api gnpsi
   transport grpc t2
      ssl profile P1
      port 7001
      authentication username priority x509-spiffe
      no disabled
```

Logs are disabled by default, including the affected facility **EosRpcAuth**.To mitigate CVE-2026-73457, ensure the facility **EosRpcAuth** status is set to disabled. The command below can be used to restore all Gnpsi agent tracing to its default setting.

```
switch(config)# no trace Gnpsi setting
```

Should it be determined that sensitive information has been logged, the affected log files must be truncated and any compromised secrets rotated to prevent gNPSI client credentials leaking.

Use the following commands to clean up Gnpsi log files:

```
switch(config)# bash sudo truncate -s 0 /var/log/agents/Gnpsi*
```

Then use the following commands to clean up previously rotated old log files:

```
switch(config)# bash sudo find /var/log/agents -name 'Gnpsi*.gz' -type f -delete
```

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-2026-73456 and CVE-2026-73457 have been fixed in the following releases:

- 4.36.2F 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

Hotfix

There is no hotfix 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