Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-73464
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: 8.7
(CVSS:4.0/AV:N/AC:L/AT:N/PR:L/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 1602598, BUG 1966288 (DMF)

Description

On affected platforms running Arista EOS with gRPC Network Management Interface (gNMI) enabled, a specially crafted request could allow a malicious authenticated client with gRPC Network Management Interface (gNMI) access to execute arbitrary code with root privileges on the switch.

This issue was discovered internally by Arista, and the company is not aware of any malicious exploitation of this vulnerability in customer networks.

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

- 4.36.0.1F and below releases in the 4.36.x train
- 4.35.5M and below releases in the 4.35.x train
- 4.34.7M and below releases in the 4.34.x train
- 4.33.8M and below releases in the 4.33.x train
- All releases in 4.32.x, 4.31.x, 4.30.x and 4.29.x trains

Impact on DANZ Monitoring Fabric (DMF)

DANZ Monitoring Fabric (DMF) deploys a fixed version of Arista EOS on certain managed fabric

switches. If the EOS version bundled with a DMF release falls within the affected version range of this advisory, DMF deployments using EOS-based switch platforms may be impacted.

DMF fabric switches running Switch Light OS are not affected by this vulnerability.

Customers running DMF should run the following command on the controller to identify the EOS version bundled with their deployment.

```
DMF-CONTROLLER> show version details
...
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ Platform files ~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
File
Hcl supported Platform
-------------------------------------------------------------------------------------
|-------------|----------------------------|
...
EOS-4.36.2F
-49446791.volgarel.1-x86_64.swi                                            True
    x86_64-7289-eos
EOS-4.36.2F-49446791.volgarel.1-x86_64.swi
 True          i686-7289-eos
EOS-4.36.2F-49446791.volgarel.1-x86_64.swi
 False         x86_64-ccs-720df-48y-eos
```

Affected Platforms

The following products **are** affected by this vulnerability:

- 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:

- Arista Wireless 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-2026-73464, the following condition must be met:

gNMI transport must be enabled

```
switch(config)#show management api gnmi
Transport: default
Enabled: yes
Server: running on port 6030, in default VRF
SSL profile: none
QoS DSCP: none
Connection limit: 100
Authorization required: no
Accounting requests: no
Notification timestamp: last change time
Listen addresses: ::
Authentication username priority: x509-spiffe, metadata, x509-common-name
Config-commands AAA accounting: enabled
Config-commands AAA authorization: enabled
```

If a gNMI transport is not configured there is no exposure to this issue and the message will look something like:

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

Indicators of Compromise

Exploitation of this vulnerability may produce error messages in the Octa or OpenConfig agent logs. The following log pattern in /var/log/agents/Octa-* or /var/log/agents/OpenConfig-* may indicate an exploitation attempt:

```
Jan 1 00:00:41 GNOI PacketLinkQual: error from pyclient
```

These messages can be found with the following commands from the bash shell:

```
[admin@Switch ~]$ grep "GNOI PacketLinkQual: error from pyclient" /var/log/agents/Octa-*
[admin@Switch ~]$ grep "GNOI PacketLinkQual: error from pyclient" /var/log/agents/OpenConfig-*
```

Note that a successful exploitation may not produce any log messages. The absence of these messages does not confirm the device was not compromised.

Mitigation

The workaround is to disable any gNMI transports.

```
management api gnmi
   no transport grpc <name>
```

Disabling all gNMI transports makes gNMI, gNOI, and gNSI services unavailable. If no RESTCONF or NETCONF transports are configured, the OpenConfig/Octa agent will also stop. CloudVision provisioning via TerminAttr is unaffected. All services resume when a gNMI transport is re-enabled.

Note: This mitigation is not applicable to DMF-managed EOS switches. gNMI transports are enabled by default on these platforms and cannot be disabled.

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-2026-73464 has been fixed in the following releases:

- 4.36.1F and later releases in the 4.36.x train
- 4.35.6M and later releases in the 4.35.x train
- 4.34.7.1M and later releases in the 4.34.x train
- 4.33.9M and later releases in the 4.33.x train

Hotfix

No hotfix is available 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