Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-73463
CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N)
CVSSv4.0 Base Score: 6.0
(CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization
This vulnerability is being tracked by BUG 1602636

Description

On affected platforms running Arista EOS, when multiple gRPC Network Security Interface (gNSI) transports are configured, a race condition in the gNSI Authz service may cause a policy rotation to fail silently. An authenticated user whose access was revoked by the new policy may retain unauthorized access to gRPC interfaces. This does not affect Bootz.

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
- 4.32.11M and below releases in the 4.32.x train
- 4.31.10M and below releases in the 4.31.x train

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-2026-73463, gNSI Authz must be enabled with multiple transports configured:

```
switch#show man api gnsi
Transport: default
Transport enabled: yes
Server: running on port 6030, in default VRF

Transport: other
Transport enabled: yes
Server: running on port 6031, in default VRF

Acctz enabled: no
Attestz enabled: no
Authz enabled: yes
Certz enabled: no
Credentialz enabled: no
Enrollz enabled: no
Pathz enabled: no
```

Please note that a system may have been affected by this vulnerability if a secondary transport (such as the "other" transport in the preceding example) was configured at *any* point. The running configuration on the system may have subsequently been modified to remove this secondary transport. Please refer to the Indicators of Compromise section below to verify the definitive evidence.

Indicators of Compromise

The bug can result in an incorrect active Authz policy. To check the active policy, run:

```
#bash sudo cat /persist/sys/gnsi/authz/policy.json
```

Mitigation

Restrict the set of users that can enable gNSI on OpenConfig / Octa transports via the CLI. We don’t support enabling gNSI via gNMI.Set.

Firstly, configure AAA authorization. The following is an example of configuring AAA authorization for all privilege levels using only the local user database:

```
switch(config)#aaa authorization commands all default local
switch(config)#aaa authorization config-commands
```

Now restrict a sufficient subset of all roles from enabling gNSI services. In the below example, we prohibit just network-operators:

```
switch(config-mgmt-api-gnsi)#role network-operator
switch(config-role-network-operator)#10 deny mode mgmt-api-
gnsi command transport gnmi .*
256 permit command .*
```

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-2026-73463 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