Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release
1.1	September 22, 2026	CSAF JSON file added

The CVE-ID tracking this issue: CVE-2026-73445
CVSSv3.1 Base Score: 4.9 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N)
CVSSv4.0 Base Score: 6.9
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-20: Improper Input Validation
This vulnerability is being tracked by BUG 1602625

Description

On affected platforms running Arista EOS, an issue with the gRPC Network Security Interface (gNSI) Authz Rotate RPC may cause an incorrect Authz policy which was uploaded in the ongoing RPC stream to become active. This does not affect Bootz.

This issue was discovered internally by Arista and the company is not aware of any malicious uses of this issue 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 the 4.31.x and 4.32.x trains

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 Serie
    - 7500R/R2/R3 Series
    - 7800R3/R4 Series
    - 7700R4 Series
    - AWE 5000 Series
    - AWE 7200R Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab

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

- Arista EOS-based products:
    - CloudVision eXchange, virtual or physical appliance
- 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-2026-73445, gNSI Authz must be configured on an OpenConfig gRPC transport:

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

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

Indicators of Compromise

Ultimately, this bug results in the active Authz policy not matching the intended policy, which should be the most recently finalized Authz policy. To see the active policy, enter:

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

If the policy looks unexpected, see when it was last written.

```
switch#bash stat /persist/sys/gnsi/authz/policy.json | grep Modify
Modify: 2026-06-25 03:11:12.901728237 -0700
```

To confirm that this bug has occurred when the active policy was last modified, there are two steps. Firstly, we assume the below tracing is configured at the time of the request.

```
switch(config)#trace OpenConfig setting log.gNSI.authz/1
switch(config)#trace Octa setting log.gNSI.authz/1
switch(config)#trace OpenConfig setting service/1
switch(config)#trace Octa setting service/1
```

Then, there will be a log at roughly the file modification time stating that a backup policy has been restored. We also search for when the corresponding Rotate RPC started, which will be the log just above the restoring backup log. In the below example, OpenConfig is configured:

```
switch#show agent OpenConfig logs | grep -e "Authz Rotate request" -e "Restoring back
up file"
I0609 03:11:11.883524   25490 service.go:236] gNSI.authz: Authz Rotate request
I0609 03:11:12.718665   25490 service.go:122] gNSI.authz: Restoring backup file
```

Now that we have confirmed that restoring a backed up policy likely corresponds to when the active policy was last written, and we have the start time of the corresponding Rotate RPC, we consider the second condition.

We assume accounting is enabled for the OpenConfig / Octa transport that received the Rotate RPC. Then, for this bug to have occurred, the last two Authz Rotate accounting records before the backup log time must be uploadRequests, and not finalizeRotations. In the below example, we search for accounting records between Rotate RPC start time and backup log time, and see that user “bob” has included two UploadRequests in the Rotate request:

```
switch#show logging time-range Jan 25 03:11:11 Jun 25 03:11:12
 | grep "gnsi.authz.v1.Authz\/Rotate"
Jun 25 03:11:12 switch Aaa: %ACCOUNTIN
G-6-CMD: bob
 gRPC %addr stop task_id=10 start_time=1782382272.580028 timezone=PDT service=shell p
riv-lvl=0 cmd=OpenConfig.Set addr=%addr:%port rpc=/gnsi.authz.v1.Authz/Rotate request
=}, redacted=[policy] <cr>
Jun 25 03:11:12 switch Aaa: %ACCOUNTING-6-CMD: bob gRPC %addr stop task_id=10 start_t
ime=1782382272.671325 timezone=PDT service=shell priv-lvl=0 cmd=OpenConfig.Set addr=%
addr:%port rpc=/gnsi.authz.v1.Authz/Rotate request=}, redacted=[policy] <cr>
```

To enable accounting for an OpenConfig / Octa transport:

1. Enable AAA accounting. Here is an example of writing accounting records to syslog:

```
switch(config)#aaa accounting commands all default start-stop logging
```

2. Enable accounting in the transport. In the below example, we use transport ‘default’:

```
switch(config)#management api gnmi
switch(config-mgmt-api-gnmi)#transport grpc default
switch(config-gnmi-transport-default)#accounting requests
```

More generally, to see whether this bug has occurred in the past (regardless of whether it’s responsible for writing the currently active Authz policy), we can carry out the same search for all "gNSI.authz: Restoring backup file” logs.

Mitigation

1. Include exactly one UploadRequest in a gNSI Authz Rotate request. For more information on the gNSI Authz Rotate RPC, see https://www.arista.com/en/support/toi/eos-4-31-0f/18445-support-for-gnsi-grpc-network-security-interface#rotate-rpc.
2. Use a gNSI Authz policy that restricts gNSI Authz use to only those who strictly need it. Below is an example policy that only allows user “Neo” to rotate Authz policies.

```
{
   "name":"restrict-authz-policy",
   "allow_rules":[
      {
         "name":"neoallow",
         "request":{
            "paths":[
               "/gnsi.authz.v1.Authz/Rotate"
            ],
            "headers":[
               {
                  "key":"username",
                  "values":[
                     "Neo"
                  ]
               }
            ]
         }
```

```
      },
      {
         "name":"allow-gnmi",
         "request":{
            "paths":[
               "/gnmi.gNMI/*"
            ]
         }
      },
      {
         "name":"allow-gnoi",
         "request":{
            "paths":[
               "/gnoi.*"
            ]
         }
      }
   ]
}
```

Ideally, this policy would be uploaded via a gNSI client for correct *version* and *created-on* metadata handling. However, we can also write directly to the active policy file, like in the following example:

```
switch#bash timeout 100 echo "]}},},}]}" | sudo tee /persist/sys/gnsi/authz/po
licy.json && sleep 11
```

For more information on gNSI Authz, see https://www.arista.com/en/support/toi/eos-4-31-0f/18445-support-for-gnsi-grpc-network-security-interface#authz.

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-2026-73445 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
- 4.34.8M 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