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-2026-73447
CVSSv3.1 Base Score: 9.1 (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H)
CVSSv4.0 Base Score: 9.4
(CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-78 OS Command Injection
This vulnerability is being tracked by BUG 1602632

Description

A vulnerability in the gRPC Network Security Interface (gNSI) Certz service on Arista EOS-based products allows an authenticated user to escalate its privilege to execute arbitrary OS commands via a crafted Certz Rotate request. The Bootz service is also affected.

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 the 4.32.x train
- All releases in the 4.31.x train
- 4.30.2F and later releases in the 4.30.x train

Affected Platforms

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

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
  - 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

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

- 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-2026-73447, gNSI Certz must be configured:

```
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: no
Certz enabled: yes
Credentialz enabled: no
Enrollz enabled: no
Pathz enabled: no
```

Or the system must use Bootz for initial provisioning.

Indicators of Compromise

auditd can be configured to monitor process creation like in the following snippet:

```
switch(config)#monitor security audit
switch(config-audit)#rule group process-creation
Enter audit rules line by line. Type 'EOF' on its own line to end.
-a always,exit -F arch=b64 -S execve -k process-create
-a always,exit -F arch=b32 -S execve -k process-create
EOF
switch(config-audit)#monitor group process-creation
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

Run the following command in bash to search for suspicious **openssl** child processes spawned by OpenConfig/Octa(assuming the OpenConfig/Octa process has pid 123):

```
$ sudo grep 'comm="openssl"' /var/log/audit/audit.log | grep "ppid=$(pgrep -f 'OpenCo
nfig|Octa')"
type=SYSCALL msg=audit(1781879247.291:20228): arch=c000003e syscall=59 success=yes ex
it=0 a0=55d56ebdbae
0 a1=55d56ebd7fd0 a2=55d56ebd8120 a3=8
 items=2 ppid=123
 pid=17285 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tt
y=(none) ses=4294967295 comm="openssl" exe="/usr/bin/openssl" key="process-create"
```

Note: Legitimate system certificate rotations may, but unlikely, spawn openssl processes. Correlate findings with unauthorized gNSI Rotate RPC calls or unexpected administrative activity before concluding exploitation occurred.

Mitigation

There is one mitigation for Bootz:

- Do not include any Certificates (X509 PEM data) when sending the initial CertzProfile via Bootz.

There are two mitigations for the Certz service:

1. Disable gNSI Certz. This fully mitigates the bug from affecting gNSI Certz, but will require manual ssl profile management. For more information on ssl profile management, see https://www.arista.com/en/support/toi/eos-4-15-0f/13673-ssl-certificate-and-key-management.
2. Use a gNSI Authz policy that restricts gNSI Certz use to only those who strictly need it. This doesn't fully mitigate the bug, but allows for the use of gNSI Certz. Firstly, enable gNSI Authz:

```
switch(config)#management api gnsi
switch(config-mgmt-api-gnsi)#service authz
```

Then, upload a strict policy. Below is an example policy that restricts Certz's Rotate RPC to user "Neo".

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
{
   "name":"restrict-certz-policy",
   "allow_rules":[
      {
         "name":"neocertz",
         "request":{
            "paths":[
               "/gnsi.authz.v1.Certz/Rotate"
            ],
            "headers":[
               {
                  "key":"username",
                  "values":[
                     "Neo"
                  ]
               }
            ]
         }
      },
      {
         "name":"neoauthz",
         "request":{
            "paths":[
               "/gnsi.authz.v1.Authz/Rotate"
            ],
            "headers":[
               {
                  "key":"username",
                  "values":[
                     "Neo"
                  ]
               }
            ]
         }
      },
      {
         "name":"allow-gnmi",
         "request":{
            "paths":[
               "/gnmi.gNMI/*"
            ]
         }
      },
      {
         "name":"allow-gnoi",
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
         "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/policy.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-2026-73447 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

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

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

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.