Date: May 6, 2025

Revision	Date	Changes
1.0	May 6, 2025	Initial release
1.1	May 20, 2025	Updated affected Arista products Updated mitigation option #3

The CVE-ID tracking this issue: CVE-2025-0936
CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N)
Common Weakness Enumeration: CWE-256: Plaintext Storage of a Password
This vulnerability is being tracked by BUG 1045796

Description

On affected platforms running Arista EOS with a gNMI transport enabled, running the gNOI File TransferToRemote RPC with credentials for a remote server may cause these remote-server credentials to be logged or accounted on the local EOS device or possibly on other remote accounting servers (i.e. TACACS, RADIUS, etc).

Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.33.0F and 4.33.1F
- 4.32.4M and below releases in the 4.32.x train
- 4.31.6M and below releases in the 4.31.x train
- From 4.30.1F through 4.30.9M in the 4.30.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

- 7010 Series
- 7010X Series
- 7020R Series
- 7130 Series running EOS
- 7150 Series
- 7160 Series
- 7170 Series
- 7050X/X2/X3/X4 Series
- 7060X/X2/X4/X5/X6 Series
- 7250X Series
- 7260X/X3 Series
- 7280E/R/R2/R3 Series
- 7300X/X3 Series
- 7320X Series
- 7358X4 Series
- 7368X4 Series
- 7388X5 Series
- 7500E/R/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 Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI - cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- 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)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2025-0936, one or both of the following conditions must be met:

- OpenConfig must be enabled with a gNOI server with accounting enabled
- OpenConfig must be enabled with a gNOI server with tracing enabled which includes any of:
    - service/9
    - interceptor/9
    - transport_socketcli/9

If OpenConfig is enabled with a gNOI server with accounting enabled, this will be shown in the following CLI output:

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

If OpenConfig is not configured or OpenConfig is configured with no gNOI server, then there is no exposure to this issue and the message will look like.

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

To see the tracing enabled for OpenConfig, run:

```
switch(config)#show running-config section trace | grep OpenConfig
trace OpenConfig setting service/9,interceptor/9,transport_socketcli/9
```

Note: gRPC-based streaming via TerminAttr to CloudVision is not affected by this vulnerability.

Indicators of Compromise

If OpenConfig is enabled with a gNOI server with accounting enabled, then this vulnerability may be indicated by the presence of lines which log RPC requests of the type “/gnoi.file.File/TransferToRemote”. For example, if logging is configured to log with syslog to /var/log/messages, then /var/log/messages may contain:

```
<DATE> <HOST> Aaa: %ACCOUNTING-6-CMD: <RPC-CALLER> gRPC <ADDRESS> stop task_id=16 sta
rt_time=<TIME> timezone=PST service=shell priv-
lvl=0 cmd=OpenConfig.Set addr=<ADDRESS> r
pc=/gnoi.file.File/TransferToRemote request=,"sourceAddress":"<REMOTE-SERVER-
ADDRESS>"}} <cr>
```

Where USERNAME and PASSWORD are the credentials for the REMOTE-SERVER-ADDRESS

If OpenConfig is enabled with a gNOI server with relevant tracing enabled, then this vulnerability may be indicated by the presence of any of the following strings in the OpenConfig agent logs:

```
GNOI File TransferToRemote: received request
```

or:

```
"method":"runCmds","params":,{"cmd":"copy file:
```

or:

```
gnoi.file.TransferToRemoteRequest:
```

These logs are visible with the command:

```
switch#show agent OpenConfig logs
```

Mitigation

There are a number of possible workarounds:

Option 1 - disable accounting/logging for the OpenConfig transport

For example to disable accounting for transport named “default”:

```
switch(config)#management api gnmi
switch(config-mgmt-api-gnmi)#transport grpc default
switch(config-gnmi-transport-default)#no accounting requests
```

to disable logging for the OpenConfig agent, run:

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

Option 2 - disable the gNOI File service entirely

To disable the gNOI File service, override the OCGNOIFileToggle, then restart OpenConfig to load the changes

```
switch#bash timeout 100 echo "OCGNOIFileToggle=0" >> /mnt/flash/toggle_override
switch#agent OpenConfig terminate
```

Disabling the gNOI File service will mean that gNOI clients will no longer be able to call any gNOI File RPCs

Option 3 - block the TransferToRemote RPC using gNSI Authz

For releases with gNSI Authz (EOS 4.31.0F and later releases), the TransferToRemote RPC can be blocked using gNSI Authz.

First enable gNSI Authz service by adding the following config:

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

Next update the authz policy to block access to the TransferToRemote RPC. This can be done directly on the system by updating the Authz policy file and waiting at least 10 seconds for OpenConfig to reload the changes:

```
switch#bash timeout 100 echo "],\"deny_rules\":[}]}" | sudo tee /persist/sys/gnsi/aut
hz/policy.json && sleep 11
```

This will cause attempts to run the TransferToRemote RPC to fail with a “PermissionDenied” error code.

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-2025-0936 has been fixed in the following releases:

- 4.30.10M and later releases in the 4.30.x train
- 4.31.7M and later releases in the 4.31.x train
- 4.32.5M and later releases in the 4.32.x train
- 4.33.2F and later releases

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