Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

Description

On affected platforms running Arista EOS, under certain circumstances plaintext private keys (CVE-2026-73465), user passwords (CVE-2026-73466) or the shared secrets for configured Terminal Access Controller Access-Control System Plus (TACACS+) servers (CVE-2026-73467) may be written to the log files during operations.

To exploit these vulnerabilities, a malicious actor must already possess authenticated local administrative access to the device shell, and specialized non-standard debugging trace levels must be explicitly enabled.

The CVE-IDs tracking these issues are:

CVE-2026-73465

CVSSv3.1 Base Score: 6.3 (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 6.0 (CVSS:4.0/AV:L/AC:H/AT:N/PR:H/UI:P/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-532: Insertion of Sensitive Information into Log File
This vulnerability is being tracked by BUG 1540441, BUG 1966285 (DMF)

CVE-2026-73466

CVSSv3.1 Base Score: 6.3 (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 6.0 (CVSS:4.0/AV:L/AC:H/AT:N/PR:H/UI:P/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-532: Insertion of Sensitive Information into Log File
This vulnerability is being tracked by BUG 1595866, BUG 1966285 (DMF)

CVE-2026-73467

CVSSv3.1 Base Score: 6.3 (CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 6.0 (CVSS:4.0/AV:L/AC:H/AT:N/PR:H/UI:P/VC:H/VI:N/VA:N/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-532: Insertion of Sensitive Information into Log File
This vulnerability is being tracked by BUG 1595862, BUG 1966285 (DMF)

These issues were 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

- 4.36.1F and earlier releases in the 4.36.x train
- 4.35.4M and earlier releases in the 4.35.x train
- 4.34.7M and earlier releases in the 4.34.x train
- 4.33.9M and earlier releases in the 4.33.x train
- All releases in the 4.32.x train
- All releases in the 4.31.x train

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
  - 7010 Series
  - 7010X Series
  - 7020R/R4 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/R4 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
  - 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 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)
- Arista DANZ Monitoring Fabric (formerly Big Switch 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)
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)

Note: Hardware platforms and software versions that have reached their end of support date at the time of this advisory are excluded from this affected list.

Required Configuration for Exploitation

CVE-2026-73465

In order to be vulnerable to CVE-2026-73465, the following condition must be met:

MgmtSecuritySslCertKey trace levels 0, 3 and/or 4, on agent ConfigAgent, must be enabled.

```
switch# show trace ConfigAgent | grep MgmtSecuritySslCertKey MgmtSecuritySslCertKey e
nabled  01.34.....
```

If MgmtSecuritySslCertKey traces levels 0, 3 and 4 are disabled, there is no exposure to this issue and the message will look something like:

```
switch# show trace ConfigAgent | grep MgmtSecuritySslCertKey MgmtSecuritySslCertKey e
nabled  ..........
```

CVE-2026-73466

In order to be vulnerable to CVE-2026-73466, the following condition must be met:

PyServer trace level 4 on agent Aaa must be enabled. The trace setting can be any regex that matches the keyword “PyServer”. The level from the output can be 4 or any range that includes 4, e.g. “0-7” or “*”.

This is an example showing the trace setting “Py*” with level with “0-5”, which will leak the password:

```
switch# show run section trace | grep Aaa
trace Aaa setting Py*/0-5
```

CVE-2026-73467

In order to be vulnerable to CVE-2026-73467, the following condition must be met:

Tacacs trace level 6 on agent Aaa must be enabled. The trace setting can be any regex that matches the keyword “Tacacs”. The level from the output can be 6 or any range that includes 6, e.g. “0-7” or “*”.

This is an example showing the trace setting “Tacacs*” with level with “0-7”, which will leak the password:

```
switch# show run section trace | grep Aaa
trace Aaa setting Tacacs*/0-7
```

Indicators of Compromise

CVE-2026-73465

This vulnerability may lead to exposed private keys on log files. As such, the following messages may appear at /var/log/agents/ConfigAgent-*:

```
2026-05-07 02:42:18.537932 18813 MgmtSecuritySslCertK 3 validateRsaPrivateKey start:
-----BEGIN RSA PRIVATE KEY-----
```

```
2026-05-07 02:42:18.537932 18813 MgmtSecuritySslCertK 3 _getPemCount start: -----BEGI
N EC PRIVATE KEY-----
```

These messages can be found with the following grep command, when run from the bash shell:

```
switch# grep "MgmtSecuritySslCertK" /var/log/agents/ConfigAgent-* | grep "PRIVATE KEY
---"
```

CVE-2026-73466

This vulnerability may lead to exposed plaintext user passwords on log files. As such, the following messages may appear at /var/log/agents/Aaa-*:

```
2026-05-11 12:48:55.366802 11172 PyServer 4 Thr_PySession59-fd16 thread _handleInput:
 b"?2\x00\x00\x001AaaApi.continueAuthenticateExec(11, '<the password>')"

2026-05-11 12:48:55.370182 11172 PyServer 4 Writing RpcStream response: b'OKid\x0011\
x00status\x00success\x00style0\x00invalid\x00text0\x00\x00style1\x00invalid\x00text1\
x00\x00style2\x00invalid\x00text2\x00\x00style3\x00invalid\x00text3\x00\x00user\x00te
stUser\x00authToken\x00<the password>' (145 bytes)

2026-05-11 12:48:55.370220 11172 PyServer 4 Thr_PySession59-fd16 write( b'\x00\x00\x0
0\x91OKid\x0011\x00status\x00success\x00style0\x00invalid\x00text0\x00\x00style1\x00i
nvalid\x00text1\x00\x00style2\x00invalid\x00text2\x00\x00style3\x00invalid\x00text3\x
00\x00user\x00testUser\x00authToken\x00<the password>' )
```

CVE-2026-73467

This vulnerability may lead to exposed TACACS+ shared key on log files. As such, the following messages may appear at /var/log/agents/Aaa-*:

```
2026-06-11 18:17:22.326396 11082 Tacacs              6 addServer: 1.2.3.4 : 1234 ns:
 default vrf: default srcIP:  srcIp6:  ke
y: <shared key> timeout: 5 flags: 0 tls: False
```

Mitigation

The workaround for all three issues involves disabling certain agent tracing levels

Caution: Disabling these levels will result in the loss of all messages generated at those levels for the given agents.

CVE-2026-73465

The workaround is to disable MgmtSecuritySslCertKey tracing on agent ConfigAgent.

```
switch(config)# no trace ConfigAgent enable MgmtSecuritySslCertKey levels 0 3 4
```

CVE-2026-73466

The workaround is to disable PyServer level 4 tracing on agent Aaa.

```
switch(config)# no trace Aaa enable PyServer levels 4
```

CVE-2026-73467

The workaround is to disable Tacacs level 6 tracing on agent Aaa.

```
switch(config)# no trace Aaa enable Tacacs levels 6
```

Clean Up Existing Log Files

If any of the above agent logging levels have been enabled, it's necessary to clean up the existing log files to remove the already leaked secrets and keys.

Use the following commands to clean up Aaa or ConfigAgent log files:

```
switch(config)# bash sudo truncate -s 0 /var/log/agents/Aaa*
switch(config)# bash sudo truncate -s 0 /var/log/agents/ConfigAgent*
```

Then use the following commands to clean up previously rotated old log files:

```
switch(config)# bash sudo find /var/log/agents -name 'Aaa*.gz' -type f -delete
switch(config)# bash sudo find /var/log/agents -name 'ConfigAgent*.gz' -type f -delet
e
```

Detection using CloudVision

An AlertBase rule has been written to detect the impacted systems; affected systems will be listed in the Compliance Dashboard. CVaaS users will have this rule automatically available in their tenants. For on-prem CloudVision clusters, additional data must be streamed to the cluster from EOS devices to enable this rule to detect affected systems.

Using a service account token, issue the following curl command to the primary node of the cluster:

```
curl -sS -kX POST --header 'Accept: application/json' -b access_token=`cat <access_to
ken>` 'https://<cluster node IP>/api/v3/services/tastreaming.TerminattrStreaming/Subs
cribeTAPaths' -d '}'
```

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-2026-73465, CVE-2026-73466 and CVE-2026-73467 have been fixed in the following releases:

- 4.36.2F and later releases in the 4.36.x train
- 4.35.5M and later releases in the 4.35.x train
- 4.34.8M and later releases in the 4.34.x train
- 4.33.10M and later releases in the 4.33.x train

Hotfix

No hotfixes are available for these issues.

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