Date: June 3, 2026

Revision	Date	Changes
1.0	June 3, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-10040
CVSSv3.1 Base Score: 6.0 (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H)
CVSSv4.0 Base Score: 6.8
(CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-348: Use of Less Trusted Source
This vulnerability is being tracked by BUG1315802

Description

A user with local ***eos-admin*** privileges on affected Arista EOS (Extensible Operating System) platforms where secure boot is enabled can bypass Secure Boot Software Image (SWI) verification through the use of a specially crafted file.

Risk Considerations: Exploitation requires existing local administrative access (***PR:H, AV:L***), meaning this vulnerability cannot be targeted remotely or by unauthenticated users.

This issue was discovered internally by Arista, and we are not aware of any malicious exploitation of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.35.1 and below releases in the 4.35.x train
- 4.34.5M and below releases in the 4.34.x train
- 4.33.7M and below releases in the 4.33.x train
- 4.32.9M and below releases in the 4.32.x train
- 4.31.10M and below releases in the 4.31.x train
- 4.30.10M and below releases in the 4.30.x train

Affected Platforms

Please refer to the “Required Configuration for Exploitation” section below as the most reliable way to determine if the system is affected.

The following products **are** affected by this vulnerability:

- Arista EOS-based products:
    - 7289-SUP-D
    - 7300-SUP2-D
    - 7388-SUP
    - CCS-710P-12
    - CCS-710P-16P
    - CCS-720DF-48Y
    - CCS-720DF-48Y-2F
    - CCS-720DF-48Y-DC
    - CCS-720DF-48Y-DC-2F
    - CCS-720DP-24S
    - CCS-720DP-24S-2F
    - CCS-720DP-24ZS
    - CCS-720DP-24ZS-2F
    - CCS-720DP-48S
    - CCS-720DP-48S-2F
    - CCS-720DP-48ZS
    - CCS-720DP-48ZS-2F
    - CCS-720DT-24S
    - CCS-720DT-24S-2F
    - CCS-720DT-24S-2R
    - CCS-720DT-48S-2F
    - CCS-720DT-48S-2R
    - CCS-720XP-96ZC2
    - CCS-722XPM-48Y4
    - CCS-722XPM-48ZY8
    - CCS-750-SUP100
    - CCS-750-SUP25
    - DCS-7010TX-48
    - DCS-7010TX-48-DC
    - DCS-7010TX-48C
    - DCS-7010TX-48C-DC
    - DCS-7010TX-48C-DC-RV3
    - DCS-7050CX3-32C
    - DCS-7050CX3M-32S
    - DCS-7050CX4-24D8
    - DCS-7050CX4M-48D8
    - DCS-7050DX4-32S
    - DCS-7050DX4M-32S
    - DCS-7050PX4-32S
    - DCS-7050SDX4-48D8
    - DCS-7050SPX4-48D8
    - DCS-7050SX3-48C8
    - DCS-7050SX3-48C8C
    - DCS-7050SX3-48YC8
    - DCS-7050SX3-48YC8C

- DCS-7050SX3-96YC8
- DCS-7050TX3-48C8
- DCS-7060CX5-56D8
- DCS-7060DX5-32
- DCS-7060DX5-64
- DCS-7060DX5-64E
- DCS-7060DX5-64S
- DCS-7060PX5-64E
- DCS-7060X6-32PE-N
- DCS-7130B-32QD
- DCS-7130LBR-48S6QD
- DCS-7132LB-48Y4C
- DCS-7135LB-48Y4C
- DCS-7170B-64C
- DCS-7280CR3-32D4
- DCS-7280CR3-32D4-M
- DCS-7280CR3-32P4
- DCS-7280CR3-32P4-M
- DCS-7280CR3-36S
- DCS-7280CR3-96
- DCS-7280CR3A-24D12
- DCS-7280CR3A-32S
- DCS-7280CR3A-48D6
- DCS-7280CR3A-72
- DCS-7280CR3AK-24D12
- DCS-7280CR3AK-32S
- DCS-7280CR3AK-48D6
- DCS-7280CR3AK-72
- DCS-7280CR3AM-24D12
- DCS-7280CR3AM-32S
- DCS-7280CR3AM-48D6
- DCS-7280CR3AM-72
- DCS-7280CR3K-32D4
- DCS-7280CR3K-32D4A
- DCS-7280CR3K-32P4
- DCS-7280CR3K-32P4A
- DCS-7280CR3K-36A
- DCS-7280CR3K-36S
- DCS-7280CR3K-96
- DCS-7280CR3MK-32D4
- DCS-7280CR3MK-32D4S
- DCS-7280CR3MK-32P4
- DCS-7280CR3MK-32P4S
- DCS-7280DR3-24
- DCS-7280DR3-24-M
- DCS-7280DR3A-36
- DCS-7280DR3A-54

- DCS-7280DR3AK-36
- DCS-7280DR3AK-54
- DCS-7280DR3AM-36
- DCS-7280DR3AM-54
- DCS-7280DR3K-24
- DCS-7280PR3-24
- DCS-7280PR3-24-M
- DCS-7280PR3K-24
- DCS-7280SR3-40YC6
- DCS-7280SR3-48YC8
- DCS-7280SR3A-48YC8
- DCS-7280SR3AK-48YC8
- DCS-7280SR3AM-48YC8
- DCS-7280SR3E-40YC6
- DCS-7280SR3E-40YC6-M
- DCS-7280SR3K-48YC8
- DCS-7280SR3K-48YC8A
- DCS-7280SR3M-48YC8
- DCS-7280TR3-40C6
- DCS-7800-SUP
- DCS-7800-SUP1A
- DCS-7816-SUP
- 7289-SUP-S-D
- AWE-5310
- AWE-5510
- AWE-7220RP-5TH-2S
- AWE-7230R-4TX-4S
- AWE-7250R-16S
- CCS-710XP-12TH-2S
- CCS-720DF-48Y-M-S-2F
- CCS-720DP-24S-M-S-2F
- CCS-720DP-48S-M-S-2F
- CCS-720DT-24S-M-S-2F
- CCS-720XP-48TXH-2C-S
- CCS-720XP-96ZC2-M-S
- CCS-720XPM-48TH-6SY
- DCS-7001-SUP-A
- DCS-7050SX3-24YC4C-S
- DCS-7050X4-48Y-4DF
- DCS-7060X6-32PE
- DCS-7060X6-64PE
- DCS-7280CR3AK-24D12-S
- DCS-7280CR3MK-32D4A-S
- DCS-7280DR3AK-36S
- DCS-7280R4-32DE
- DCS-7280R4-32PE
- DCS-7280R4-64QC-10PE

- DCS-7280R4K-32DE
- DCS-7280R4K-32PE
- DCS-7280R4K-64QC-10PE
- DCS-7280SR3MK-48YC8A-S
- DCS-7800-SUP1S
- DCS-7816-SUP1S
- ZTX-7230S-4TX-4S
- ZTX-7250S-16S

Additional information can be found at https://www.arista.com/assets/data/pdf/platform-specific-security-features-guide.pdf

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

- Arista EOS-based products:
  - 7300-SUP
  - 7300-SUP-D
  - 7326-56X-O-AC
  - 7368-SUP
  - 7368-SUP-D
  - 7388-SUP-D
  - 7726-32X-O-AC
  - CCS-720XP-24Y6
  - CCS-720XP-24ZY4
  - CCS-720XP-48Y6
  - CCS-720XP-48ZC2
  - DCS-7020SR-24C2
  - DCS-7020SR-32C2
  - DCS-7020SRG-24C2
  - DCS-7020TR-48
  - DCS-7020TRA-48
  - DCS-7050CX3-32S
  - DCS-7050CX3-32S-SSD
  - DCS-7050SX3-48YC12
  - DCS-7060CX-32C
  - DCS-7060CX-32S
  - DCS-7060CX2-32S
  - DCS-7060DX4-32
  - DCS-7060DX4-32C-RV3
  - DCS-7060DX4-32S
  - DCS-7060DX4-32SB-RV3
  - DCS-7060PX4-32
  - DCS-7060SX2-48YC6
  - DCS-7130-16G3
  - DCS-7130-16G3S

- DCS-7130-48E
- DCS-7130-48EH
- DCS-7130-48EHS
- DCS-7130-48G3
- DCS-7130-48G3S
- DCS-7130-48L
- DCS-7130-48LA
- DCS-7130-48LAS
- DCS-7130-48LB
- DCS-7130-48LBA
- DCS-7130-48LBAS
- DCS-7130-48LBS
- DCS-7130-48LS
- DCS-7130-96
- DCS-7130-96E
- DCS-7130-96L
- DCS-7130-96LA
- DCS-7130-96LAS
- DCS-7130-96LB
- DCS-7130-96LBA
- DCS-7130-96LBAS
- DCS-7130-96LBS
- DCS-7130-96LS
- DCS-7130-96S
- DCS-7170-32C
- DCS-7170-32C-M
- DCS-7170-32CD
- DCS-7170-64C
- DCS-7170-64C-M
- DCS-7260CX-64
- DCS-7260CX-64-SSD
- DCS-7260CX3-64
- DCS-7260CX3-64E
- DCS-7260CX3-64LQ
- DCS-7260QX-64
- DCS-7260QX-64-SSD
- DCS-7280CR-48
- DCS-7280CR2-60
- DCS-7280CR2A-30
- DCS-7280CR2A-60
- DCS-7280CR2K-30
- DCS-7280CR2K-60
- DCS-7280CR2M-30
- DCS-7280QR-C36
- DCS-7280QR-C36-M
- DCS-7280QR-C72
- DCS-7280QR-C72-M

    - DCS-7280QRA-C36S
    - DCS-7280QRA-C36S-M
    - DCS-7280SR-48C6
    - DCS-7280SR-48C6-M
    - DCS-7280SR2-48YC6
    - DCS-7280SR2-48YC6-M
    - DCS-7280SR2A-48YC6
    - DCS-7280SR2A-48YC6-M
    - DCS-7280SR2K-48C6-M
    - DCS-7280SRA-48C6
    - DCS-7280SRA-48C6-M
    - DCS-7280SRAM-48C6
    - DCS-7280SRM-40CX2
    - DCS-7280TR-48C6
    - DCS-7280TR-48C6-M
    - DCS-7280TRA-48C6
    - DCS-7280TRA-48C6-M
    - DCS-7500-SUP2
    - DCS-7500-SUP2-D
    - DCS-7516-SUP2
    - DCS-7516-SUP2-D
- 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)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2026-10040, Secure Boot must be actively supported and enabled on the platform.

Secure boot must be enabled:

```
# enable
# show boot | grep “Secure boot”
Secure boot: enabled
```

If secure boot is not enabled or not supported, there is no exposure to this issue and the message will look like:

```
# enable
# show boot | grep “Secure boot”
Secure boot: disabled
```

Or:

```
# enable
# show boot | grep “Secure boot”
```

If the output displays ***Secure boot: disabled*** or returns no text output , the system is not exposed to this vulnerability.

Indicators of Compromise

Due to the nature of this vulnerability, no reliable indicators of compromise exist. Integrity validation relies on the underlying platform hardware architecture upon subsequent secure remediated boots.

Mitigation

There are no runtime mitigation options available for this issue. Security exposure is entirely dependent on restricting administrative access to authorized personnel. Remediation requires a software upgrade.

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_token>` 'https://<cluster node IP>/api/v3/services/tastreaming.TerminattrStreaming/SubscribeTAPaths' -d '}'
```

Above steps would be needed to be executed on on-prem CVP so that BugAlerts can flag the devices impacted.

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.

Note: Applying these software updates requires a standard switch reload, which will result in a temporary network disruption. Arista recommends scheduling these updates during a regular maintenance window.

For more information about upgrading see EOS User Manual: Upgrades and Downgrades

CVE-2026-10040 has been fixed in the following releases:

- 4.32.10M and later releases in the 4.32.x train
- 4.33.8M and later releases in the 4.33.x train
- 4.34.6M and later releases in the 4.34.x train
- 4.35.2F and later releases in the 4.35.x train

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