Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-73451
CVSS:3.1 Base Score: 4.8 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N)
CVSS:4.0 Base Score: 6.3
(CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-1419: Incorrect Initialization of Resource
This vulnerability is being tracked by BUG1262274

Description

On affected platforms running Arista EOS with dual switch cards and with ingress Security ACLs configured on Switched Virtual Interfaces (SVI) in shared mode, restarting of the secondary switchcard forwarding agent or insertion of secondary switchcard, can cause security ACLs on shared SVIs to stop functioning. This may result in incorrect packet permit/deny behavior.

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
- 4.35.4M and below releases in the 4.35.x train
- 4.34.6M and below releases in the 4.34.x train
- 4.33.8M and below releases in the 4.33.x train
- 4.32.11M and below releases in the 4.32.x train
- Releases between 4.31.1F to 4.31.10M in the 4.31.x train

Affected Platforms

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

- Arista EOS-based products:
  - 755 Series
  - 758 Series

The following product versions and platforms **are not** 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 Series
  - 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
- Wi-Fi 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-2026-73451, the following condition must be met:

Security ACL must be configured on SVI in ingress direction, which by default uses a shared ACL identifier. In the example below RACLID = 1 for both switchcards:

```
switch>show run interface vlan
interface Vlan100
   ip access-group acl1 in

switch>show platform trident tcam acl
=== IP ACLs on switch SwitchcardCes1/0 ===

INGRESS ACL acl1 uses 2 entries
    Assigned to VLANs: 100
    Shared ACL Identifier (RACLID): 1
    Assigned to ports: None

=== MAC ACLs on switch SwitchcardCes1/0 ===

=== IPv6 ACLs on switch SwitchcardCes1/0 ===

=== IP ACLs on switch SwitchcardCes2/0 ===

INGRESS ACL acl1 uses 2 entries
    Assigned to VLANs: 100
    Shared ACL Identifier (RACLID): 1
    Assigned to ports: None

=== MAC ACLs on switch SwitchcardCes2/0 ===

=== IPv6 ACLs on switch SwitchcardCes2/0 ===
```

If Security ACL is **not** configured on SVI in ingress direction, there is no exposure to this issue and the message will look something like:

```
switch>show run interface vlan
interface Vlan100

switch>show platform trident tcam acl
=== IP ACLs on switch SwitchcardCes1/0 ===

=== MAC ACLs on switch SwitchcardCes1/0 ===

=== IPv6 ACLs on switch SwitchcardCes1/0 ===

=== IP ACLs on switch SwitchcardCes2/0 ===

=== MAC ACLs on switch SwitchcardCes2/0 ===

=== IPv6 ACLs on switch SwitchcardCes2/0 ===
```

Indicators of Compromise

This vulnerability may result in incorrect packet filtering on an SVI with an ingress security ACL, potentially causing packets that should be permitted to be denied, or packets that should be denied to be permitted.

Mitigation

The workaround is to re-configure (remove and reapply) the ingress IPv4 and IPv6 ACLs applied to all SVIs.

For every SVI check the active ACL(s) applied to it,

```
switch(config)# interface VlanNNN
switch(config-if-VlNNN)# show active
```

Then remove the ACL(s) and re-apply them,

```
switch(config-if-VlNNN)# no ip access-group <acl name> in
switch(config-if-VlNNN)# ip access-group <acl name> in
```

```
switch(config-if-VlNNN)# no ipv6 access-group <acl name> in
switch(config-if-VlNNN)# ipv6 access-group <acl name> in
```

Note: the security provided by the ACL configuration will not be present during the removal/reapplication of the security ACLs.

For more information about Security ACLs see EOS User Manual: ACLs and Route Maps.

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-2026-73451 has been fixed in the following releases:

- 4.36.1F and later release in the 4.36.x train
- 4.35.5M and later releases in the 4.35.x train
- 4.34.7M and later releases in the 4.34.x train
- 4.33.9M and later releases in the 4.33.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