Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-73468
CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 7.1
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L)
Common Weakness Enumeration: CWE-670: Always-Incorrect Control Flow Implementation
This vulnerability is being tracked by BUG 1857585

Description

On affected Arista EOS platforms configured with Protocol Independent Multicast (PIM) Sparse Mode, a specially crafted packet can cause the premature expiry of multicast forwarding state on affected interfaces. This may result in temporary loss of multicast traffic forwarding during the affected period.

This issue was discovered internally by Arista, and Arista is not aware of any malicious uses of this issue 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 below releases in the 4.36.x train
- 4.35.5M and below releases in the 4.35.x train
- 4.34.7.1M and below releases in the 4.34.x train
- 4.33.8M and below releases in the 4.33.x train
- 4.32.x and earlier versions are affected

Affected Platforms

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

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
- 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 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-2026-73468 , the following condition must be met:

The attack surfaces are interfaces with PIM Sparse Mode configured. PIM interfaces can belong to default or non-default VRFs. Both IPv4 and IPv6 modes are vulnerable.

For example:

```
switch(config)# interface Ethernet1
switch(config-if-Et1)# pim ipv4 sparse-mode

switch# show pim ipv4 sparse-mode interface
Address      Interface  Mode   Neighbor Hello  DR DR Address  PktsQed PktsDropped
                               Count Intvl Pri
------------ ---------- ------ -------- ----- --- ----------- ------- -----------
172.17.26.1  Ethernet1  sparse        1    30   1 172.17.26.1       0           0

switch(config)# interface Vlan2
switch(config-if-Vl2)# vrf blue
switch(config-if-Vl2)# pim ipv6 sparse-mode

switch# show pim ipv6 vrf blue sparse-mode interface
Address      Interface  Mode   Neighbor Hello  DR DR Address  PktsQed PktsDropped
                               Count Intvl Pri
------------ ---------- ------ -------- ----- --- ----------- ------- -----------
10::20::1    Vlan2      sparse        1    30   1 10::20::1         0           0
```

If PIM Sparse Mode is not configured, there is no exposure to this issue and the message will look something like:

```
switch(s2)#show pim ipv4 sparse-mode interface
% ipv4 multicast routing is not configured on VRF blue.

switch(s2)#show pim ipv6 vrf blue sparse-mode interface
% ipv6 multicast routing is not configured on VRF default.
```

Indicators of Compromise

This vulnerability may lead to unexpected blackholing of multicast traffic destined for downstream routers and receivers.

The "**show pim [vrf VRFNAME] sparse-mode route [group] [source]**" command may show potential signs of misbehavior if the route is missing or has unexpectedly low uptime.

In the following example, the customer expects 3 multicast routes (10.0.0.10, 10.0.0.20, 10.0.0.30). However, multicast traffic streams sourced from 10.0.0.20 and 10.0.0.30 were affected. The 10.0.0.20 stream is still affected, missing from the CLI output, while the 10.0.0.30 stream has recovered a few seconds ago, with a low uptime.

```
switch#show pim ipv4 sparse-mode route
...
225.1.1.1
  10.0.0.10, 3:21:08, flags: SLP
    Incoming interface: Ethernet1
    RPF route: [U] 10.0.0.10/32 [0/0]
    Outgoing interface list:
      Ethernet2
      Ethernet3
  10.0.0.30, 0:0:03, flags: SLP
    Incoming interface: Ethernet3
    RPF route: [U] 10.0.0.30/32 [0/0]
    Outgoing interface list:
      Vlan20
```

Mitigation

There is no mitigation available to address this vulnerability. For the final resolution, please refer to the next section which lists the details of the remediated software versions.

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-2026-73468 has been fixed in the following releases:

- 4.36.2F and later releases in the 4.36.x train
- 4.35.6M and later releases in the 4.35.x train
- 4.34.8M and later releases in the 4.34.x train
- 4.33.9M and later releases in the 4.33.x train

Hotfix

No hotfixes are available for this issue

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