Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release
1.1	September 17, 2026	Moved 7368X4 Series to Affected
1.2	September 22, 2026	CSAF JSON file added

The CVE-ID tracking this issue: CVE-2026-77190
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: 6.0
(CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L
Common Weakness Enumeration: CWE-20 Improper Input Validation
This vulnerability is being tracked by BUG 1852734

Description

On affected platforms running Arista EOS, an unauthenticated attacker who is network-adjacent to the switch and able to connect to a device with PIM Sparse Mode and MLAG configured, can send malformed messages that cause the Pimsm agent to terminate unexpectedly. The Pimsm agent is automatically restarted, but repeated attacks can cause the agent to restart continuously, resulting in a sustained denial of service.

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

- 4.36.1F and earlier releases in the 4.36.x train
- 4.35.5M and earlier releases in the 4.35.x train
- Releases between 4.34.2F and 4.34.7M in the 4.34.x train

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

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 Series
  - 7500R/R2/R3 Series
  - 7800R3/R4 Series
  - cEOS-lab
  - vEOS-lab

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

- Arista EOS-based products:
  - 7700R4 Series
  - AWE 5000 Series
  - AWE 7200R Series
  - CloudEOS
  - 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)

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

- 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-2026-77190, the following conditions must be met:

1. PIM Sparse Mode must be configured. This could be for IPv4 or IPv6. For example:

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

switch# show agent Pimsm uptime
  Agent Name         Restarts              Uptime
------------------ ------------- ----------------
Pimsm                        1    2 days, 14:00:28

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

switch# show agent Pimsm6 uptime
  Agent Name         Restarts              Uptime
------------------ ------------- ----------------
Pimsm6                       3    2 days, 14:00:20
```

2. MLAG must be configured and active.

```
switch(config)# mlag
switch(config-mlag)# local-interface vlan 4094
switch(config-mlag)# peer-address 10.0.0.2
switch(config-mlag)# peer-link port-channel 10
switch(config-mlag)# domain-id mlag1
```

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

```
switch# show mlag
MLAG Configuration:
domain-id : mlag1
local-interface : Vlan4094
peer-address : 10.0.0.2
peer-link : Port-Channel10
MLAG Status:
state : Active
peer-link status : Up
local-int status : Up
system-id : 00:11:22:01:03:01
```

Indicators of Compromise

Exploitation of this vulnerability may result in the affected agent restarting repeatedly. Unexpected agent restarts of the Pimsm agent may be an indication of the issue, and can appear in the output of **show logging** as messages similar to:

```
Jan 1 00:00:41 switch ProcMgr-worker: %PROCMGR-6-... Restarting Pimsm immediately
```

Mitigation

There is no mitigation or workaround available.

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-2026-77190 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

Hotfix

There is no hotfix available for this issue.

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

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

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.