Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release
1.1	September 22, 2026	CSAF JSON file added

The CVE-ID tracking this issue: CVE-2026-73438
CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 7.0
(CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-617: Reachable Assertion
This vulnerability is being tracked by BUG 1876199

Description

On affected platforms running Arista EOS with Open Shortest Path First version 3 (OSPFv3) configured, an unauthenticated attacker on the same OSPFv3 broadcast domain can send a specially crafted set of packets that can cause the Ospf3 agent to restart unexpectedly. The crash results in the loss of all OSPFv3 adjacencies on the affected device and may disrupt routing across the broader OSPF domain until the agent recovers.

This issue was reported externally by Dravanet Inc., and Arista 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 below releases in the 4.36.x train
- 4.35.5M and below releases in the 4.35.x train
- 4.34.7M and below releases in the 4.34.x train
- 4.33.9M and below releases in the 4.33.x train
- All prior releases

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
  - 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:

- 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 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-2026-73438, the following condition must be met:

OSPFv3 must be configured:

```
switch>show ospfv3
OSPFv3 address-family ipv4
Routing Process "ospfv3" with ID 10.1.1.5 and Instance 64 VRF default
...
OSPFv3 address-family ipv6
Routing Process "ospfv3" with ID 10.1.1.5 and Instance 0 VRF default
...
```

or

```
switch>show ipv6 ospf
Routing Process "ospfv3 0" with ID 10.1.1.5 and Instance 0 VRF default
...
```

If the commands produce no output, then OSPFv3 is not configured:

```
switch>show ospfv3
switch>show ipv6 ospf
```

Indicators of Compromise

This vulnerability may lead to the Ospf3 agent restarting unexpectedly on the switch.

If you see the following message in show logging:

```
Jan 1 00:00:00 switch ProcMgr: %PROCMGR-6-PROCESS_TERMINATED: 'Ospf3' (PID=11997, sta
tus=-11) has terminated.
Jan 1 00:00:00 switch ProcMgr: %PROCMGR-3-PROCESS_DELAYRESTART: 'Ospf3' (PID=11997) r
estarted too often! Delaying restart for 180.0 (until 0000-01-01 00:04:00.893496)
```

Mitigation

The OSPFv3 authentication feature helps to mitigate this vulnerability. OSPFv3 authentication prevents unauthorized actors from injecting crafted packets into the OSPF domain. Enabling it on all OSPFv3-speaking interfaces ensures that packets from unauthenticated senders are discarded before they can trigger this vulnerability.

Per-interface OSPFv3 encryption

Configure ESP-based encryption with authentication on each OSPFv3 interface. All peers on the same interface must use the same SPI, algorithm, and passphrase.

```
switch(config)# interface <interface-name>
switch(config-if)# ospfv3 encryption ipsec spi <spi-
value> esp aes-256-cbc sha1 passphrase <shared-passphrase>
```

Per-area OSPFv3 Configuration:

Configure ESP-based encryption with authentication on each OSPFv3 area.

```
switch(config)# router ospfv3
switch(config-router-ospfv3)# address-family ipv4
switch(config-router-ospfv3-af)# area <area-id> encryption ipsec spi <spi-
value> esp aes-256-cbc sha1 passphrase <shared-passphrase>
switch(config-router-ospfv3-af)# address-family ipv6
switch(config-router-ospfv3-af)# area <area-id> encryption ipsec spi <spi-
value> esp aes-256-cbc sha1 passphrase <shared-passphrase>
```

Caution: Enabling OSPFv3 authentication must be coordinated across peering neighbors simultaneously. Applying this configuration to a single peer will temporarily break the routing adjacency, resulting in traffic disruption

For full configuration reference, see the EOS User Manual — OSPFv3 Authentication and Encryption.

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-2026-73438 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
- 4.33.10M and later releases in the 4.33.x train

Hotfix

No hotfix is 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