**Date: September 9, 2026**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | September 9, 2026 | Initial release |

The CVE-ID tracking this issue: CVE-2026-73435
CVSSv3.1 Base Score: 8.2 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:L/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-345: Insufficient Verification of Data Authenticity
This vulnerability is being tracked by BUG 1843809

The CVE-ID tracking this issue: CVE-2026-73436
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:N)
Common Weakness Enumeration: CWE-1284: Improper Validation of Specified Quantity in Input,
CWE-125: Out-of-bounds Read CWE-125: Out-of-bounds Read
This vulnerability is being tracked by BUG 1843812

# Description

### CVE-2026-73435

On affected platforms running Arista EOS with Open Shortest Path First version 2 (OSPFv2) configured, a specially crafted OSPFv2 packet from an unauthenticated attacker on the same broadcast segment, with OSPFv2 authentication configured can cause adjacency flapping and packet loss. The disruption can affect routing across the broader OSPF domain.

### CVE-2026-73436

On affected platforms running Arista EOS with OSPFv2 and OSPFv2 segment routing configured, a specially crafted OSPFv2 packet from an adjacent OSPF neighbor may cause OSPF to restart unexpectedly.

These issues were discovered internally by Arista, and the company is not aware of any malicious uses of these issues 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

### CVE-2026-73435

#### 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

### CVE-2026-73436

#### 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
- 4.33.9M and below releases in the 4.33.x train
- All prior releases

## Affected Platforms

### CVE-2026-73435 and CVE-2026-73436

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

- Arista EOS-based products:
  - 710 Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series
  - 7010 Series
  - 7010X Series
  - 7020R/R4 Series
  - 7130 Series running EOS
  - 7150 Series
  - 7160 Series
  - 7170 Series
  - 7050X/X2/X3/X4 Series
  - 7060X/X2/X4/X5/X6 Series
  - 7250X Series
  - 7260X/X3 Series
  - 7280E/R/R2/R3/R4 Series

- 7300X/X3 Series
- 7320X Series
- 7358X4 Series
- 7368X4 Series
- 7388X5 Series
- 7500E/R/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:

- 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
- 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

### CVE-2026-73435

In order to be vulnerable to CVE-2026-73435, all of the following conditions must be met:

1. The vulnerable OSPFv2 instance must have at least two neighbors on the same interface.
2. The interface is a broadcast interface.
3. OSPFv2 cryptographic authentication is configured.

Here is an example showing a vulnerable OSPFv2 instance with a minimum of two neighbors on the same interface.

```
switch>show ip ospf neighbor
Neighbor ID Instance VRF ... Interface
X.X.X.X     X       …    ... <intf>
X.X.X.X     X       …    ... <intf>
```

Here is an example showing the vulnerable configuration of Network Type “Broadcast” and Message-digest authentication (cryptographic authentication) configured:

```
switch>show ip ospf interface
<intf> is up
  Interface Address X.X.X.X/X, instance X, VRF X, Area X.X.X.X
  Network Type Broadcast, Cost: X
  ...
  Message-digest authentication, using key id X
  ...
```

Note: Both “Message-digest authentication” ( MD5 ) and “Message-digest sha<X> authentication” ( SHA ) are vulnerable.

To check area-level authentication, reference the vulnerable interface area ID in “**show ip ospf** ” output below:

```
switch>show ip ospf
OSPF instance X with ID X.X.X.X VRF X
...
Area X.X.X.X
 Number of interface in this area is X
   It is a X area
   Traffic engineering is disabled
   Area has MD5 authentication
```

If the area has “**Simple**” or “**None**” authentication, then at the area-level, the third prerequisite

is unmet and the system would not be vulnerable to this particular issue.

### CVE-2026-73436

In order to be vulnerable to CVE-2026-73436, the following condition must be met:

OSPFv2 segment routing must be configured. If the below command shows any OSPF instance, then the deployment is vulnerable.

```
switch>show ip ospf segment-routing
SPF Instance ID: 1
...
```

If OSPFv2 segment routing is not configured, then there is no exposure to this issue.

## Indicators of Compromise

### CVE-2026-73435

This vulnerability may result in OSPF flaps.

Affected neighbor entries may flap in “**show ip ospf neighbor**”. Meaning existing neighbor entries can disappear and reappear from the list below. Other signs of flapping include re-appearing neighbors with non-full state and “**/BDR**” or “**/DR**” state migrating to other neighbors.

```
switch> show ip ospf neighbor
Neighbor ID     Instance VRF      Pri State ...
1.1.1.1         1        default  1   FULL/BDR ...
```

Syslog indicators of compromise can be found in the EOS CLI via the “**show logging**” command. If in privileged mode or higher the “**show logging**” output can be piped to the following grep commands in the EOS CLI.

```
switch# show logging | grep “OSPF-4-OSPF_ADJACENCY_TEARDOWN.\inactivity timer expired
”
```

The following log message may appear in the output of the “show logging” command:

```
11:14:19.237398 Instance 1: %OSPF-4-OSPF_ADJACENCY_TEARDOWN: NGB 1.1.1.1, interface 1
.0.0.2 adjacency dropped: inactivity timer expired, state was: FULL
```

### CVE-2026-73436

This vulnerability may lead to unexpected OSPF restarts.

Here is an example for OSPF restart log:

```
Jan 1 00:00:14 switch ProcMgr: %PROCMGR-6-PROCESS_TERMINATED: 'Ospf' (PID=1, status=1
31) has terminated.
Jan 1 00:00:14 switch ProcMgr: %PROCMGR-6-PROCESS_RESTART: Restarting 'Ospf' immediat
ely (it had PID=1)
```

These messages can be found in the EOS CLI through the "**show logging**" command. The show logging output can be piped to the following grep commands in the EOS CLI:

```
switch# show logging | grep “ProcMgr: %PROCMGR-6-PROCESS_TERMINATED: 'Ospf' (PID=.*,
status=.*)”
switch# show logging | grep "Restarting 'Ospf' immediately"
```

## Mitigation

No mitigation is available for both CVE-2026-73435 and CVE-2026-73436.

## 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-2026-73435

CVE-2026-73435 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
- 4.34.7.1M and later releases in the 4.34.x train
- 4.33.10M and later releases in the 4.33.x train

### CVE-2026-73436

CVE-2026-73436 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

### CVE-2026-73435

The following hotfix can be applied to remediate CVE-2026-73435. The hotfix only applies to the releases listed below and no other releases. All other versions require upgrading to a release containing the fix (as listed above).:

- 4.36.1F
- 4.35.5M
- 4.34.7M
- 4.33.9M

Note: Installing/uninstalling the SWIX will cause the Ospf process to restart

Version: 1.0
URL: CVE-2026-73435.swix

```
SWIX hash:(SHA512)
4c4ff053d8165f347b45dfcafc2d20396e3eb00869b0088f3128be7f53b2a028b479fa8279849c800b591
6ab9aaf8077718a68e3bf4277d55b44076650de0aa7
```

For instructions on installation and verification of the hotfix patch, refer to the “managing eos extensions” section in the EOS User Manual. Ensure that the patch is made persistent across reboots by running the command ‘copy installed-extensions boot-extensions’.

### CVE-2026-73436

There is no hotfix available for CVE-2026-73436. It is required to upgrade to a release containing the fix (as listed above).

### 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