Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-73455
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 8.9
(CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-130: Improper Handling of Length Parameter Inconsistency
This vulnerability is being tracked by BUG1307559

Description

On affected platforms running Arista EOS with Open Shortest Path First version 3 (OSPFv3) configured, a specially crafted packet can cause the OSPFv3 agent to restart unexpectedly. Exploitation of this vulnerability can be executed remotely over the network.

This issue was discovered internally by Arista and the company 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

- 4.36.0.1F 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
- 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 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-2026-73455, the following condition must be met:

If OSPFv3 is not configured there is no exposure to this issue and the show command will not produce any output

```
switch>show ospfv3

switch>show ospfv3 neighbor
```

To confirm if your configuration is vulnerable, execute the following commands. The vulnerability requires **both** OSPFv3 to be enabled and at least one active neighbor to be present:

```
switch>show ospfv3
Routing Process "ospfv3" with ID 192.0.2.0 and Instance 0 VRF default
...
It has 1 fully adjacent neighbors
```

```
switch>show ospfv3 neighbor
Neighbor 192.0.3.0 VRF default priority is 1, state is Full
```

Note: If OSPFv3 is not configured, the command will yield no output and your system is not exposed.

Indicators of Compromise

This vulnerability may lead to the OSPFv3 agent becoming non-responsive and eventually restarting on the switch.

The OSPFv3 process being terminated due to a SIGQUIT may be an indication of the issue.

The following message may appear in “**show logging**”.

```
Jan 1 00:00:41 switch ProcMgr: %PROCMGR-4-TERMINATE_PROCESS_SIGQUIT: Heartbeats from
'Ospf3' (PID=1) missing for 601.0 secs -- terminating it with SIGQUIT. Process kernel
 stack is (). Syscall is (running).
```

The following kernel message may also appear under “**/var/log/eos**” (this requires bash access) which indicates the issue:

```
Jan 1 00:00:14 switch ProcMgr: %PROCMGR-6-PROCESS_TERMINATED: 'Ospf3' (PID=1, status=
131) has terminated.
Jan 1 00:00:14 switch ProcMgr: %PROCMGR-6-PROCESS_RESTART: Restarting 'Ospf3' immedia
tely (it had PID=1)
```

These messages can be found with the following grep commands, when run from the bash shell:

```
$ grep “ProcMgr: %PROCMGR-6-PROCESS_TERMINATED: 'Ospf3' (PID=.*, status=.*)” /var/log
/eos
$ grep "Restarting 'Ospf3' immediately" /var/log/eos
```

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-2026-73455 has been fixed in the following releases:

- 4.36.1F and later releases 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

Hotfix

The following hotfix can be applied to remediate CVE-2026-73455. 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).:

- 4.36.0.1F
- 4.35.4M
- 4.34.6M
- 4.33.8M

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

Version: 1.0
URL: CVE-2026-73455_Hotfix.swix

```
SWIX hash:(SHA512)
8f67f7c343bce9b63a62bd359a6bbf6b6cc05cff73aae0a3f8ecefc5bc2f29645448a4b6053ab0bba96ee
b6095f1f7529e386d5dbe36fbe0e92f5afa4889dc34
```

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**'.

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