Date: December 16, 2025

Revision	Date	Changes
1.0	December 16, 2025	Initial release

The CVE-ID tracking this issue: CVE-2025-8872
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H (6.5 / 10)
CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N (7.1 / 10)
Common Weakness Enumeration: CWE-400: Uncontrolled Resource Consumption
This vulnerability is being tracked by BUG1203059

Description

On affected platforms running Arista EOS with OSPFv3 configured, a specially crafted packet can cause the OSFPv3 process to have high CPU utilization which may result in the OSFPv3 process being restarted. This may cause disruption in the OSFPv3 routes on the switch.

This issue was discovered internally by Arista and is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.34.1F and below releases in the 4.34.x train
- 4.33.4M and below releases in the 4.33.x train
- 4.32.7M and below releases in the 4.32.x train
- 4.31.8M and below releases in the 4.31.x train
- All releases prior to 4.31.x train

Affected Platforms

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

- Arista EOS-based products:
  - 710/710XP Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series
  - 7010 Series
  - 7010X Series

- 7020R 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 Series
- 7300X/X3 Series
- 7320X Series
- 7358X4 Series
- 7368X4 Series
- 7388X5 Series
- 7500E/R/R2/R3 Series
- 7700R4 Series
- 7800R3/R4 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 as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)
- 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-2025-8872, the following condition must be met:

The OSFPv3 protocol must be configured in either the default or non default vrf and at least one neighbor must be present

```
switch>show ospfv3
OSPFv3 address-family ipv6
Routing Process "ospfv3" with ID 192.0.2.0 and Instance 0 VRF default
  FIPS mode disabled
  Maximum number of LSAs allowed 0
    Exceed action disable
    LSA limit for warning message 75%
    Disabled-time 5 minutes, clear timeout 5 minutes
    Incident count 0, incident count limit 5
  It is an autonomous system boundary router and is not an area border router
  Minimum LSA arrival interval 1000 msecs
  Initial LSA throttle delay 1000 msecs
  Minimum hold time for LSA throttle 5000 msecs
  Maximum wait time for LSA throttle 5000 msecs
  It has 1 fully adjacent neighbors
  Number of areas in this router is 1. 1 normal, 0 stub, 0 nssa
  Number of LSAs 8
  Initial SPF schedule delay 0 msecs
  Minimum hold time between two consecutive SPFs 5000 msecs
  Current hold time between two consecutive SPFs 5000 msecs
  Maximum wait time between two consecutive SPFs 5000 msecs
  SPF algorithm last executed 00:04:52 ago
  No scheduled SPF
  Adjacency exchange-start threshold is 20
  Maximum number of next-hops supported in ECMP is 128
  Number of backbone neighbors is 0
  Graceful-restart is not configured
  Graceful-restart-helper mode is enabled
  Area 0.0.0.0
    Number of interface in this area is 1
    It is a normal area
    SPF algorithm executed 6 times

switch>show ospfv3 neighbor
OSPFv3 address-family ipv6
Routing Process "ospfv3" Instance 0 VRF default
Neighbor 192.0.3.0 VRF default priority is 1, state is Full
  In area 0.0.0.0 interface Ethernet4
```

```
  Adjacency was established 00:00:49 ago
  Current state was established 00:00:49 ago
  DR is 3.3.3.3 BDR is 2.2.2.2
  Options is E R V6
  Dead timer is due in 29 seconds
  Graceful-restart-helper mode is Inactive
  Graceful-restart attempts: 0
```

If OSFPv3 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
```

Indicators of Compromise

This vulnerability may lead to the OSFPv3 agent becoming non responsive and eventually restarting on the switch.

The OSFPv3 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
'OSFPv3' (PID=1) missing for 601.0 secs -- terminating it with SIGQUIT. Process kerne
l stack is (). Syscall is (running).
```

The following messages 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: 'OSFPv3' (PID=1, status
=131) has terminated.
Jan 1 00:00:14 switch ProcMgr: %PROCMGR-6-PROCESS_RESTART: Restarting 'OSFPv3' immedi
ately (it had PID=1)
```

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

```
grep "Heartbeats from 'OSFPv3' (PID=.*) missing for .* secs" /var/log/eos
grep "Restarting 'OSFPv3' immediately" /var/log/eos
```

Mitigation

There is no workaround to mitigate the issue.

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-2025-8872 has been fixed in the following releases:

- 4.34.2F and later releases in the 4.34.x train
- 4.33.5M and later releases in the 4.33.x train
- 4.32.8M and later releases in the 4.32.x train
- 4.31.9M and later releases in the 4.31.x train

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