Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-121293
CVSSv3.1 Base Score: 4.4 (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 6.9
(CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-476 NULL Pointer Dereference
This vulnerability is being tracked by BUG 1961865, 1961866

Description

On affected EOS-based platforms, an attacker who controls a Border Gateway Protocol (BGP) peer can send a crafted BGP message over an established session with the Dynamic Path Selection (DPS) address family negotiated. This can cause the BGP process to terminate unexpectedly, resetting all BGP sessions and disrupting routing services until the process restarts.

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

- 4.36.2F and below releases in the 4.36.x train
- 4.35.6M and below releases in the 4.35.x train
- 4.34.8M and below releases in the 4.34.x train
- 4.33.10M and below releases in the 4.33.x train
- All releases in the 4.32.x train
- All releases in the End of Support software release trains

Affected Platforms

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

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.

- 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/XE7 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
  - ZTX-7200 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 cloud service delivery
- CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on premises software)
- CloudVision Appliance Software
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- 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

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.

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-2026-121293, at least one BGP peer with BGP address family “path-selection” must be in an “established” state. To check, run the following show command.

```
evpnsfe1#show bgp path-selection summary
BGP summary information for VRF default
Router identifier 0.0.0.1, local AS number 300
Neighbor Status Codes: m - Under maintenance
  Neighbor V AS           MsgRcvd   MsgSent  InQ OutQ  Up/Down State   PfxRcd PfxAcc
PfxAdv
  12.0.0.3 4 300
         44        43    0    0 00:14:55 Estab   1      1      1
evpnsfe1#
```

If ALL BGP peers with the address family “path-selection” are in any other states, there is no exposure to this issue, for example in the below show commands.

1. path-selection is not configured.

```
evpnsfe1#show bgp path-selection summary
BGP summary information for VRF default
Router identifier 0.0.0.1, local AS number 300
Neighbor Status Codes: m - Under maintenance
  Neighbor V AS           MsgRcvd   MsgSent  InQ OutQ  Up/Down State   PfxRcd
PfxAcc PfxAdv
evpnsfe1#
```

2. path-selection is configured but the BGP session is not established with peer (it may be down, or BGP itself not configured in the peer).

```
evpnsfe1#show bgp path-selection summary
BGP summary information for VRF default
```

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.

```
Router identifier 0.0.0.1, local AS number 300
Neighbor Status Codes: m - Under maintenance
  Neighbor V AS           MsgRcvd   MsgSent  InQ OutQ  Up/Down State   PfxRcd
PfxAcc PfxAdv
  12.0.0.3 4 300              112       338    0    0 00:00:13 Active
evpnsfe1#
```

3. path-selection is configured, BGP session with peer is established but peer does not have path-selection configured.

```
evpnsfe1(config)#show bgp path-selection summary
BGP summary information for VRF default
Router identifier 0.0.0.1, local AS number 300
Neighbor Status Codes: m - Under maintenance
  Neighbor V AS           MsgRcvd   MsgSent  InQ OutQ  Up/Down State   PfxRcd
PfxAcc PfxAdv
  12.0.0.3 4 30
0               15        16    0    0 00:05:47 Estab(NotNegotiated)
evpnsfe1(config)#
```

Indicators of Compromise

Exploitation of this vulnerability causes the BGP process to terminate and restart. The following messages may appear in show logging:

```
%PROCMGR-6-PROCESS_TERMINATED: 'Bgp' (PID=XXXX, status=-11) has terminated.
%PROCMGR-6-PROCESS_TERMINATED: 'Bgp' (PID=XXXX, status=-6) has terminated.
%SYS-4-RESTART_SERVICE: Service Bgp is not running. Attempting to restart it.
```

These messages can be found using the following command:

```
switch#show logging | include PROCESS_TERMINATED.*Bgp
```

Repeated BGP process crashes, particularly correlating with the receipt of DPS route updates from a specific peer, may be a stronger indicator of exploitation. The BGP peer session will be re-established after each restart, potentially allowing the cycle to repeat.

Mitigation

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.

There is no mitigation available for this 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-2026-121293 has been fixed in the following releases:

- 4.37.0F and later releases in the 4.37.x train
- 4.36.3M and later releases in the 4.36.x train
- 4.35.7M and later releases in the 4.35.x train
- 4.34.9M and later releases in the 4.34.x train
- 4.33.11M and later releases in the 4.33.x train

Hotfix

No hotfix 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
- By email: support@arista.com
- By telephone: List of regional telephone numbers

Receive notification for new advisories and notices:

Subscribe to the RSS feed and email notifications to receive periodic updates on new software releases, advisories, end of sale and field notices.

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.