Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-120979
CVSSv3.1 Base Score: 8.1 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H)
CVSSv4.0 Base Score: 6.1
(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-1289: Improper Validation of Unsafe Equivalence in Input
This vulnerability is being tracked by BUG 2059581

Description

This vulnerability affects customers using Arista Pathfinder for WAN path selection with Border Gateway Protocol-Link State (BGP-LS) configured for Dynamic Path Selection (DPS). On affected platforms running Arista EOS with BGP-LS configured for DPS, an attacker who has established an authenticated BGP-LS session with the device can send a specially crafted BGP packet to cause incorrect WAN path selection and disrupt traffic forwarding.

This vulnerability 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

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.

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

- Arista EOS-based products:
  - AWE 5000 Series
  - AWE 7200R Series
  - CloudEOS

The following product versions and platforms **are not** 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/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
  - ZTX-7200 Series
  - cEOS-lab
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance
- Wi-Fi Access Points
- CloudVision CUE cloud service delivery
- CloudVision Portal, 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

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.

- 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, BGP-LS must be configured, at least one BGP-LS peer session must be established, and the device must be configured as a Pathfinder node.

1. BGP-LS configured with a peer session established:

```
switch(config)#show bgp link-state 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   NlriRcd
 NlriAcc NlriAdv

12.0.0.3 4 300
            82        83    0    0 01:02:33 Estab   0      0      1
switch(config)#
```

   And

2. The device is configured as a Pathfinder node:

```
switch#show adaptive-virtual-topology path | section Role:
Role: pathfinder
```

Not Affected:

If BGP-LS is not configured or no peers are established, the device is not vulnerable.

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.

If any one of these steps match, then the device is NOT affected.

1. BGP link-state is not configured.

```
switch(config-router-bgp)#show bgp link-state 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   NlriRcd
 NlriAcc NlriAdv
switch(config-router-bgp)#
```

2. The device is not configured in the Pathfinder role.

```
switch#show adaptive-virtual-topology path | section Role:
Role: edge

switch#show adaptive-virtual-topology path | section Role:
Role: zone transit

switch#show adaptive-virtual-topology path | section Role:
Role: region transit

switch#show adaptive-virtual-topology path | section Role:
Role: unknown
```

Indicators of Compromise

Unexpected changes in WAN path selection or traffic forwarding, without corresponding configuration changes, may indicate exploitation. Compare current and previously collected show adaptive-virtual-topology path output for changes in active paths, next-hop VTEPs, or hop lists.

Example path-state log records: A **high rate of change** of active path syslog messages may indicate exploitation.

Sample output:

```
2026-10-30 10:01:59.305918 320072 Log                    0 %SFE-6-PATH_ACTIVE: Group mp
ls path 10.1.3.1 to 10.1.5.1 (ID:4) to peer 12.0.0.5 is active for traffic class \x00
.
2026-10-30 10:01:59.306144 320072 Log                    0 %SFE-6-PATH_ACTIVE: Group in
```

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.

```
ternet path 10.2.3.1 to 10.2.5.1 (ID:8) to peer 12.0.0.5 is active for traffic class
\x00.
2026-10-30 10:02:04.309346 320072 Log                    0 %SFE-6-PATH_INACTIVE: Group
mpls path 10.1.3.1 to 10.1.5.1 (ID:4) to peer 12.0.0.5 is inactive for traffic class
\x00.
```

Commands for collecting supporting information:

```
show logging | include SFE-6-PATH_ACTIVE|SFE-6-PATH_INACTIVE
show path-selection paths
show adaptive-virtual-topology path
show adaptive-virtual-topology path detail
show adaptive-virtual-topology path counters
```

Mitigation

There are no configuration-level mitigations that fully resolve this issue without upgrading software.

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-2026-120979 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

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.

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.