Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

Description

All of the CVEs covered in this advisory apply to affected platforms running Arista EOS with the Virtual Private LAN Service using BGP Signaling (VPLS-BGP) enabled on the Provider Edge (PE) routers. These issues primarily affect customers using VPLS-BGP to connect disparate customer L2 networks.

These issues were discovered internally by Arista, and the company is not aware of any malicious exploitation of these vulnerabilities in customer networks.

CVE-2026-120980

On affected platforms running Arista EOS with VPLS-BGP enabled, an attacker who has established a BGP session with the PE routers can send a specially crafted BGP packet to cause the BGP agent to restart unexpectedly.

CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 6.0
(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:L)
Common Weakness Enumeration: CWE-617 Reachable Assertion
This vulnerability is being tracked by BUG 1925240

CVE-2026-120981

On affected platforms running Arista EOS with VPLS-BGP enabled, an attacker who has established a BGP session with the PE router can affect the route advertisements of VPLS pseudowires, causing a churn of the established routes with other legitimate BGP peers.

CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 6.0
(CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:L/SA:L)
Common Weakness Enumeration: CWE-772 Missing Release of Resource after Effective Lifetime
This vulnerability is being tracked by BUG 1925302

Vulnerability Assessment

Platform and Software Applicability Note

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.

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.

Affected Platforms

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

- Arista EOS-based products:
  - 7280R3 Series
  - 7500R3 Series
  - 7800R3 Series

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/R4 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500R/R2 Series
  - 7800R4 Series
  - 7700R4 Series

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.

    - AWE 5000 Series
    - AWE 7200R Series
    - ZTX-7200 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
- 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 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-2026-120980 or CVE-2026-120981, the following condition must be met:

VPLS using BGP signaling must be configured. The configured VPLS-BGP groups can be viewed using the show bgp vpls signaling command.

```
switch>show bgp vpls signaling
VPLS instance: CUSTOMER_1, group: BGP_MESH_1
Route distinguisher: 10.1.1.1:42
Route target to import: Route-Target-AS:65534:100
Route target to export: Route-Target-AS:65534:100
Local VE-ID: 1
Remote VE-ID: 2, address: 10.2.2.2, encap label: 116384, decap label: 136385
Remote VE-ID: 3, address: 10.3.3.3, encap label: 116385, decap label: 136386
```

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 VPLS using BGP signaling is not configured, the “show bgp vpls signaling” command should produce no output.

```
switch>show bgp vpls signaling
```

Indicators of Compromise

CVE-2026-120980

Exploitation of this vulnerability causes the BGP process to terminate and restart. When you have VPLS-BGP enabled and if the BGP process unexpectedly terminates, the following messages may appear in show logging:

```
Jan 1 00:00:00 switch ProcMgr: %PROCMGR-6-PROCESS_TERMINATED: 'Bgp' (PID=21234, statu
s=-6) has terminated.
```

CVE-2026-120981

Exploitation of this vulnerability may lead to VPLS pseudowire signaling using VPLS-BGP to fail unexpectedly for a subset of negotiated VPLS pseudowires. One or more VPLS-BGP pseudowires may unexpectedly show a signaling error rather than the negotiated pseudowire MPLS labels. An example of the show bgp vpls signaling command displaying VPLS-BGP pseudowire signaling errors is:

```
switch# show bgp vpls signaling
VPLS instance: CUSTOMER_1, group: BGP_MESH_1
Route distinguisher: 10.1.1.1:42
Route target to import: Route-Target-AS:65534:100
Route target to export: Route-Target-AS:65534:100
Local VE-ID: 1
Remote VE-ID: 2, address: 10.2.2.2, error: requested feature is not supported
Remote VE-ID: 3, address: 10.3.3.3, error: no Layer2 Info extended community received
```

Mitigation

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

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.

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-2026-120980 and CVE-2026-120981 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

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.