Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-121286
CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:N/AC:L/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:N)
Common Weakness Enumeration: CWE-476: NULL Pointer Dereference
This vulnerability is being tracked by BUG 1975990

Description

On affected platforms running Arista EOS in multi-agent routing model with BGP Segment Routing Traffic Engineering (SR-TE) address family configured, a BGP peer can send crafted BGP packets to cause the BGP process to restart, disrupting all BGP sessions on the device.

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
- End of Support software release trains between 4.22.1F and 4.31.x

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, 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-2026-121286, the following condition must be met:

Routing model is multi-agent and BGP must be configured, and either SR-TE IPv4 or SR-TE IPv6 address family is configured and there's at least one BGP neighbor established in IPv4/6 SR-TE AFI/SAFI.

```
switch# show ip route summary
...
Operating routing protocol model: multi-agent
Configured routing protocol model: multi-agent
...

switch# show bgp sr-te summary
BGP summary information for VRF default
Router identifier 192.0.2.2, local AS number 100
Neighbor Status Codes: m - Under maintenance
  Neighbor         V  AS           MsgRcvd   MsgSent  InQ OutQ  Up/Down State  PfxRcd
 PfxAcc
  192.0.2.1
      4  100          407       413      0    0   00:18:57 Estab  1      1
  2001:DB8::1
      4  100          407       413      0    0   00:18:57 Estab  1      1
```

```
switch# show ip bgp neighbors 192.0.2.1
  BGP version 4, remote router ID 192.0.2.1, VRF default
  Negotiated BGP version 4
  ...
  Neighbor Capabilities:
    Multiprotocol IPv4 Unicast: advertised and received and negotiated

Multiprotocol IPv4 Segment Routing Traffic Engineering Policy: advertised and receive
d and negotiated
```

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.

```
Multiprotocol IPv6 Segment Routing Traffic Engineering Policy: advertised and receive
d and negotiated
```

Indicators of Compromise

Exploitation of this vulnerability may result in ‘Bgp’ agent restarting repeatedly. Unexpected agent restarts of the Bgp agent may be an indication of the issue, and can appear in the output of show logging as messages similar to:

```
Jan 1 00:00:41 switch ProcMgr: %PROCMGR-6-PROCESS_TERMINATED: 'Bgp' (PID=2743, status
=-6) has terminated.
Jan 1 00:00:41 switch ProcMgr-
worker: %PROCMGR-6-PROCESS_RESTART: Restarting 'Bgp' immediately (it had PID=2743)
```

Mitigation

For complete mitigation guidance and assistance, customers are advised to contact the Arista Networks Technical Assistance Center (TAC) for support.

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-2026-121286 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

There are no hotfixes available for this issue.

For More Information

If you require further assistance, or if you have any further questions regarding this security

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.

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.