Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-121289
CVSSv3.1 Base Score: 9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 9.3
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-121: Stack-based Buffer Overflow
This vulnerability is being tracked by BUG 1927959

Description

On affected platforms running Arista EOS with BGP configured, a specially crafted packet can cause the BGP agent to crash.

Successful exploitation causes the BGP agent process to terminate, resulting in the loss of all BGP sessions on the affected device and possible disruption to network routing until the process recovers. Due to the nature of the vulnerability, it may also be possible for a sophisticated attacker to achieve arbitrary code execution, which could compromise the confidentiality and integrity of the affected system.

This issue was reported to Arista by Joshua Foote of JP Morgan Chase. Arista 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 in the 4.33.x train
- All releases in the End of Support software release trains, beginning with 4.25.1F

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.

Affected Platforms

The following products **are** 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
  - 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

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) - 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-2026-121289, the following condition must be met:

BGP must be configured AND the multi-agent routing protocol model must be in use:

```
switch>show ip bgp summary
BGP summary information for VRF default
Router identifier 10.0.0.1, local AS number 65000
Neighbor Status Codes: m - Under maintenance
  Neighbor   V  AS    MsgRcvd   MsgSent  InQ OutQ  Up/Down State   PfxRcd PfxAcc
  10.0.0.2   4  65001     100       100    0    0 01:00:00 Estab   10     10

switch>show running-config all | inc service routing protocols
service routing protocols model multi-agent
```

The vulnerable code paths are active whenever BGP is enabled and a BGP peering session is established.

If BGP is not configured OR if the multi-agent routing protocol model is not in use there is no exposure to this issue and the output will look something like:

```
switch>show ip bgp summary
% BGP is not running
switch>show run all | inc service routing protocols
service routing protocols model ribd
```

Indicators of Compromise

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 BGP agent crashing or restarting unexpectedly may be an indication of exploitation. The following log message may appear in “**show logging**”:

```
Jan 1 00:00:41 switch ProcMgr: %PROCMGR-6-PROCESS_TERMINATED: 'Bgp' (PID=<pid>, statu
s=-11) has terminated.
```

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

```
grep "PROCESS_TERMINATED: 'Bgp'" /var/log/eos
```

Mitigation

For BGP sessions that do not rely on the Tunnel Encapsulation Attribute, a workaround is to remove all received Tunnel Encapsulation Attributes by configuring attribute discard, for example:

```
neighbor default received attribute discard 23
```

Alternatively, a recommended mitigation to reduce exposure to this vulnerability is to configure BGP peer authentication using TCP-AO in order to ensure that only authorized peers can establish a BGP session.

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-2026-121289 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

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.

No hotfixes are 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.