Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release
1.1	November 12, 2026	Update Mitigation

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 releases in the 4.33.x train
- All releases in the 4.32.x train

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.

- All releases in the End of Support software release trains, beginning with 4.25.1F

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

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 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-2026-121289, 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
```

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.

Indicators of Compromise

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

BGP Attribute 23 is the Tunnel Encapsulation Attribute (RFC 9012) and is used in BGP EVPN to signal to the receiving router how to encapsulate packets (tunnel type, VNI, outer IP endpoint, color/policy) to reach the advertising Border Leaf or VTEP.

Filtering Attribute 23 at external eBGP peering edges (ISPs, transit providers, uncoordinated WANs) prevents a remote ASN from injecting overlay tunnel instructions into the local and trusted EVPN administrative domains through the Border leafs. This attribute is generally not used and should not leak in from or out to external eBGP peering edges that rely on standard IPv4 and IPv6 unicast for reachability exchange.

In EOS, the following AFI/SAFIs use the Tunnel Encapsulation Attribute:

- BGP EVPN (AFI: 25, SAFI: 70)
    - The BGP-EVPN Tunnel Encapsulation attribute supports a dual-stack IPv4/IPv6 underlay by enabling a VTEP to advertise both IPv4 and IPv6 tunnel endpoints as next hops in a single BGP update
- BGP SR Policy (AFI:1, SAFI:73)
- BGP DPS (Dynamic Path Selection) (AFI: 1/2, SAFI: 79)

For customers using the above features, please upgrade to the fixed versions to fully mitigate the vulnerability.

For BGP sessions that do not rely on the Tunnel Encapsulation Attribute (see caveats below), a workaround is to remove all received Tunnel Encapsulation Attributes by configuring attribute discard.

```
switch(config)# router bgp <ASN>
switch(config-router-bgp)# neighbor default received attribute discard 23
```

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 above commands require you to fill in a configured ASN number for <ASN>. The “neighbor default” command will apply the mitigation globally for all peers. The attribute discard can be disabled on specific peers if it is required within the customer application, using the configuration below:

```
switch(config)# router bgp <ASN>
switch(config-router-bgp)# neighbor X.X.X.X received attribute discard disabled
```

Alternatively, you can apply the attribute discard to select peers or peer-groups:

```
switch(config)# router bgp <ASN>
switch(config-router-bgp)# neighbor <X.X.X.X|peer-group-
name> received attribute discard 23
```

The above configuration will only take effect for newly received BGP updates. Running **ip clear bgp * soft in** or session reset is not required to have this take effect for new updates to existing routes. A route refresh or reset is required to make “attribute discard” effective for existing routes to ensure the use of this attribute has been removed from existing routes.

Please note important caveats with the use of “attribute discard” command:

- There is a known issue, BUG1030490, where high route churn and attribute discard may cause a Bgp agent restart. This issue was introduced in EOS 4.29.2 and is fixed in EOS 4.30.10, 4.31.8, 4.32.5, 4.33.3 and 4.34.1.
- There is a known issue, BUG2082773, where attribute 255 should not be configured to be discarded. Discarding this attribute can cause the Bgp agent to restart under certain circumstances. This issue will be fixed in upcoming releases.

To verify that attributes are being discarded run **show ip[v6] bgp neighbors|peers** and verify that the output shows “configured received path attribute types to discard” includes “23”. For example:

```
switch# show ip bgp neighbors
BGP neighbor is 10.0.0.2, remote AS 2, external link    ...    Inbound updates with a
ttribute errors:
    Resulting in removal of all paths in update (treat as withdraw): 0
    Resulting in AFI/SAFI disable: 0
    Resulting in attribute ignore: 0
    Disabled AFI/SAFIs: None
```

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.

```
Configured received path attribute types to discard: 23    Attribute Type Updates wit
h Discards
  ------------- --------------------
              23                    4
  Inbound paths dropped by reason:
    IPv4 unicast NLRIs dropped due to martian prefix: 0
    IPv6 unicast NLRIs dropped due to martian prefix: 0
    IPv4 labeled-unicast NLRIs dropped due to excessive labels: 0
    IPv4 labeled-unicast NLRIs dropped due to martian prefix: 0
    IPv6 labeled-unicast NLRIs dropped due to excessive labels: 0
   ...
```

The above shows that BGP update packets with attribute type 23 have been discarded 4 times.

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

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

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.

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.