Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-121290
CVSSv3.1 Base Score: 8.2 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H)
CVSSv4.0 Base Score: 8.3
(CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-420: Unprotected Alternate Channel
This vulnerability is being tracked by BUG 1977472

Description

On affected platforms running Arista EOS with Border Gateway Protocol (BGP) changing the BGP listen port from its default value disables default protective Access Control List (ACL) rules against unexpected BGP peering attempts.

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
- All releases in the End of Support software release trains

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-2026-121290, the following conditions must all be met:

1. The BGP listen port must be set to a non-default value (something other than TCP port 179):

```
switch>show running-config section bgp | include listen-port
  bgp transport listen-port 1179
```

2. The multi-agent routing protocol model must be in use:

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

If either of the above outputs are missing there is no exposure. There is no ACL protection that drops incoming TCP connections from unexpected remote IP addresses which makes DOS attacks more effective. If Generalized TTL Security Mechanism (GTSM) is configured, the GTSM rules that implement TTL checks are rendered ineffective.

Indicators of Compromise

There are no direct log-based indicators of compromise for this vulnerability. The issue manifests as a silent absence of GTSM ACL rules rather than a logged error.

When the problem is present, the ACL rules are observed to use the default port, 179, in the following output:

```
switch#bash sudo iptables -L -n | grep -a "EOS_BGP "
Chain EOS_BGP (2 references)
EOS_BGP    tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:179
EOS_BGP    tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:179
rvt304#bash sudo ip6tables -L -n | grep -a "EOS_BGP "
Chain EOS_BGP (2 references)
```

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.

```
EOS_BGP    tcp      ::/0                ::/0                tcp spt:179
EOS_BGP    tcp      ::/0                ::/0                tcp dpt:179
switch#
```

When the problem is not present, the non-default port (1179 in this example) is observed in the same output:

```
switch#bash sudo iptables -L -n | grep -a "EOS_BGP "
Chain EOS_BGP (2 references)
EOS_BGP    tcp  --  0.0.0.0/0           0.0.0.0/0           tcp spt:1179
EOS_BGP    tcp  --  0.0.0.0/0           0.0.0.0/0           tcp dpt:1179
rvt304#bash sudo ip6tables -L -n | grep -a "EOS_BGP "
Chain EOS_BGP (2 references)
EOS_BGP    tcp      ::/0                ::/0                tcp spt:1179
EOS_BGP    tcp      ::/0                ::/0                tcp dpt:1179
switch#
```

Mitigation

If operationally feasible, removing the non-default listen port configuration allows protecting to be effective on the default BGP port (179):

```
router bgp <asn>
   no bgp transport listen-port
```

If the non-default listen port must be retained, the required modifications to the control plane ACL (to allow the non-default listen port to be reached) should be made in such a manner to provide the desired protection — only allowing TCP connections using the non-default listen port when the remote IP address in an expected one, and if applicable, when the TTL value is within the expected range.

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-2026-121290 has been fixed in the following releases:

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.

- 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

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.