Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-121369
CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)
CVSSv4.0 Base Score: 6.7
(CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-770: Allocation of Resources Without Limits or Throttling
This vulnerability is being tracked by BUG 1880613

Description

On affected platforms running Arista EOS under specific link configurations an attacker with direct connectivity to the system may cause system CPU and memory utilization to increase considerably leading to slow responsiveness and eventually may cause the system to reboot.

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

- 4.36.1M and below releases in the 4.36.X train
- 4.35.6M and below releases in the 4.35.X train
- 4.34.2F through 4.34.7M releases in the 4.34.x train

Affected Platforms

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

- Arista EOS-based products:
  - 750X 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.

    - CCS-750XM-48TX-LC
    - CCS-750XPM-48NH-LC
    - CCS-750XPM-48TXH-LC

The following product versions and platforms **are not** affected by this vulnerability:

- Arista EOS-based products:
    - 710 Series
    - 720D Series
    - 720XP/722XPM 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
- 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

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 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-2026-121369, the following condition must be met:

The interfaces on the affected linecard must be set to either speed auto or no speed (default). To verify run the following show commands:

```
switch(config-if-Et3/1)#show active all | grep speed
   no speed

switch(config-if-Et3/2)#show active
interface Ethernet3/2
   speed auto
```

If no interfaces are configured with “speed auto” or “no speed”, the device is not exposed to this issue.

Indicators of Compromise

This vulnerability may lead to elevated memory utilization, high CPU usage, or out-of-memory conditions on the switch.

Sustained high memory or CPU utilization by the StrataQosV2 or StrataFabric processes may be an early indication of this issue, as in the example below.

```
switch(config)# show processes top once
top - 00:37:55 up  2:14,  4 users,  load average: 8.53, 8.02, 7.07
Tasks: 339 total,  13 running, 326 sleeping,   0 stopped,   0 zombie
%Cpu(s): 82.1 us,  3.2 sy,  0.0 ni, 14.3 id,  0.0 wa,  0.4 hi,  0.0 si,  0.0 st
MiB Mem :  15865.8 total,   3644.0 free,   9568.6 used,   3733.6 buff/cache
MiB Swap:      0.0 total,      0.0 free,      0.0 used.   6297.2 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 5692 root      20   0    9.9g   2.8g 137260 R  98.3  18.3  58:54.12 StrataQosV2
```

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.

```
5685 root      20   0 9386256   1.4g 110456 R  97.7   9.2  64:02.73 StrataFabric
4238 root      20   0 9695972 658612 342276 S   0.7   4.1   7:59.28 ConfigAgent
```

Mitigation

The workaround is to configure an explicit speed on all interfaces. As an example the following command can be used to apply an explicit speed on an interface:

```
switch(config)# interface Ethernet3/2
switch(config-if-Et3/2)# speed auto 1g
```

To verify the change has been applied, you can use the following show command:

```
switch(config)# interface Ethernet3/2
switch(config-if-Et3/2)#show active
interface Ethernet3/2
   speed auto 1g
```

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-2026-121369 has been fixed in the following releases:

- 4.37.0F and later releases in the 4.37.x train
- 4.36.2M and later releases in the 4.36.X train
- 4.35.7M and later releases in the 4.35.X train
- 4.34.7.1M and later releases in the 4.34.X train

Hotfix

No hotfix 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.