Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-121370
CVSSv3.1 Base Score: 8.6 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)
CVSSv4.0 Base Score: 9.2
(CVSS:4.0/AV:N/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 1860051

Description

On affected platforms running Arista EOS with Precision Time Protocol (PTP) configured, an unauthenticated attacker with network access to a PTP-enabled port can create a denial of service (DoS) condition by sending traffic to the system.

This issue was discovered internally by Arista and is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.34.1F and below releases in the 4.34.x train
- 4.33.8M 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 in the 4.31.x and 4.30.x trains
- 4.29.2F and later in the End of Support software in the 4.29.x release train

Affected Platforms

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

- Arista EOS-based products:
  - 750X Series

The following product versions and platforms **are not** 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
  - 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
- 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)

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.

- 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-2026-121370, the following condition must be met:

PTP must be configured globally, and there must be at least one interface enabled, verify by running the below show command.

```
switch>show ptp
PTP Mode: Boundary Clock
PTP Profile: Default ( IEEE1588 )
Clock Identity: XX:XX:XX:XX:XX:XX:XX:XX
Grandmaster Clock Identity: XX:XX:XX:XX:XX:XX:XX:XX
Number of slave ports: 0
Number of master ports: 1
Offset From Master (nanoseconds): 0
Mean Path Delay (nanoseconds): 0
Steps Removed: 0
Skew (estimated local-to-master clock frequency ratio): 1.0
   Interface       State        Transport    Delay
                                             Mechanism
-------------- ------------ --------------- ---------
   Et1             Master       ipv4         e2e
```

If PTP is not configured there is no exposure to this issue and the message will look something like:

```
switch>show ppt
PTP Mode: Disabled
```

Indicators of Compromise

Exploitation of this vulnerability results in high CPU utilization and may prevent other control-plane traffic from being processed by the CPU.

To check whether the PTP CPU queue is receiving an abnormal volume of traffic, run the following command in privileged EOS CLI mode:

```
switch# platform trident Linecard* diag show c  | grep PERQ_PKT.*cpu0
```

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.

```
PERQ_PKT(1).cpu0  :       4,753                +3,422                2/s
PERQ_PKT(1).cpu0  : 253,990,371         +183,850,577          130,829/s
```

The rightmost column of the PERQ_PKT(1).cpu0 indicates a high volume of traffic on the PTP CPU queue and may be evidence of exploitation.

Note: the absence of these indicators does not rule out exploitation.

Mitigation

A bandwidth limit can be applied to the PTP CPU queue to prevent CPU saturation by running the following commands in the privileged EOS CLI mode.

```
switch# platform trident Linecard* diag mod MMU_MAX_BUCKET_QLAYER 1 1 THD_SEL=0x4d RE
FRESH=0x28
switch# platform trident Linecard* diag mod MMU_MIN_BUCKET_QLAYER 1 1 THD_SEL=0x10 RE
FRESH=0x8
```

Note: If PTP is currently enabled on any interfaces, disable it on those interfaces before running the mitigation commands, then re-enable it afterward.

To disable PTP on an interface, run the following command in the privileged EOS CLI configuration mode.

```
switch(config-if)# no ptp enable
```

Note: These settings are not persistent. They must be re-applied after any forwarding plane reset or line card replacement.

To verify the results of these configurations, run the following commands in privileged EOS CLI:

```
switch# platform trident Linecard* diag d chg MMU_MIN_BUCKET_QLAYER.mmu0 1 1
```

The output should be similar to the following:

```
Linecard1/0 :
MMU_MIN_BUCKET_QLAYER.mmu0[1]: <THD_SEL=0x10,REFRESH=8,>
Linecard1/1 :
```

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.

```
MMU_MIN_BUCKET_QLAYER.mmu0[1]: <THD_SEL=0x10,REFRESH=8,>
...
```

Then run:

```
switch# platform trident Linecard* diag d chg MMU_MAX_BUCKET_QLAYER.mmu0 1 1
```

The output should be similar to the following:

```
Linecard1/0 :
MMU_MAX_BUCKET_QLAYER.mmu0[1]: <THD_SEL=0x4d,REFRESH=0x28,>
Linecard1/1 :
MMU_MAX_BUCKET_QLAYER.mmu0[1]: <THD_SEL=0x4d,REFRESH=0x28,>
...
```

The mitigation is correctly applied, if each line card slot listed produces exactly one output line and THD_SEL, and REFRESH matches the examples above.

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-2026-121370 has been fixed in the following releases:

- All releases in trains 4.35.x, 4.36.x and 4.37.x
- 4.34.2F and later releases in the 4.34.x train
- 4.33.9M and later releases in the 4.33.x train

Hotfix

No hotfix is 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

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.

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.