Date: November 20, 2026

Revision	Date	Changes
1.0	November 20, 2026	Initial release
1.1	November 20, 2026	Correct typo in impacted EOS version

The CVE-ID tracking this issue: CVE-2026-99288
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
Common Weakness Enumeration: CWE-476 - Null Pointer Dereference
This vulnerability is being tracked by BUG2077060 (EOS), BUG2089900 (VCO/VCG)

Description

Arista Networks is providing this security update in response to a vulnerability affecting the use of IPv4 in the Linux kernel. It is believed to be possible to allow an unauthenticated attacker to cause a kernel panic (crash and restart) in the kernel if exploited by sending traffic to a reachable TCP port. This issue is colloquially known as “NoisyTCP”.

This issue is a publicly disclosed vulnerability in open source software, 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

- 4.37.0F
- 4.36.3.2M and earlier releases in the 4.36.X train
- 4.35.7.2M and earlier releases in the 4.35.X train
- 4.34.9.2M and earlier releases in the 4.34.X train
- 4.33.11.2M and earlier releases in the 4.33.X train
- All releases in the End of Support software release trains going back to 4.21.3F

VeloCloud Orchestrator Versions

- 7.0.0.3 and below releases in the 7.0.0 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.

- 6.4.2.16 and below releases in the 6.4.2 train
- 6.1.3.13 and below releases in the 6.1.3 train
- 5.2.3.20 and below releases in the 5.2.3 train

VeloCloud Edge and Gateway Versions

- 7.0.0.0 and below releases in the 7.0.0 train
- 6.4.4.2 and below releases in the 6.4.x train
- 6.1.6.2 and below releases in the 6.1.x train
- 5.2.7.2 and below releases in the 5.2.x train

Wi-Fi Access Points

- 22.4.0M and below releases in the 22.0.0 train
- 21.7.0M and below releases in the 21.0.0 train
- All releases in the End of Support software release train going back to 20.0.0 train

CloudVision Appliance Software Versions

- 7.2.0 and below releases

Impact on DANZ Monitoring Fabric (DMF)

DANZ Monitoring Fabric (DMF) deploys a fixed version of Arista EOS on certain managed fabric switches. If the EOS version bundled with a DMF release falls within the affected version range of this advisory, DMF deployments using EOS-based switch platforms may be impacted.

DMF fabric switches running Switch Light OS are not affected by this vulnerability.

Customers running DMF should run the following command on the controller to identify the EOS version bundled with their deployment.

```
DMF-CONTROLLER> show version details
...
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ Platform files ~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
File                                                
```

```
EOS-4.36.2F-49446791.volgarel.1-x86_64.swi
 False          x86_64-ccs-720df-48y-eos
```

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 5000/7200R Series
  - ZTX-7200 Series
  - cEOS-lab
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance
- CloudVision Appliance Software
- 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)
- VeloCloud Orchestrator (Formerly VeloCloud Orchestrator by Broadcom)
- VeloCloud Gateway (Formerly VeloCloud Gateway by Broadcom)
- VeloCloud Edge (Formerly VeloCloud Edge by Broadcom)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly

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.

Untangle)
- CloudVision CUE cloud service delivery
- CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on premises software)
- CloudVision as-a-Service
- CloudVision Sensor
- Wi-Fi Access Points
    - Wi-Fi6/6E AP series (C200, C230, O235, C250, C260, C360, C330, W318 and their variants)
    - Wi-Fi7 AP series (C400, O405, C430, O435, C460 and their variants)

Unaffected Platforms

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

- Arista EOS Based Products:
    - CloudEOS
    - AWE Series
- Wi-Fi Access Points
    - WiFi5 AP series (C100, C110, W118, C120, C130, O105 and their variants)

Under Triage

The following product versions and platforms **are undergoing triage** to determine if they are affected by this vulnerability:

- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)

Required Configuration for Exploitation

All vulnerable products without specific subsections below are vulnerable due to internal settings. No configuration controls if they are vulnerable or not.

VeloCloud Edge

The impact of this CVE on VeloCloud Edge (VCE) is limited due to the following reasons:

- Management services are not reachable from the WAN by default.
- When administrators enable these services, access is limited to the source addresses or LAN interfaces they configure.

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.

- Tunnel traffic is not affected. SD-WAN overlay traffic uses UDP encapsulation and is not processed by Linux.

It is recommended to keep Edge Access settings for SSH, local web UI and SNMP at their default of disabled. Where they are needed, restrict them to specific trusted source addresses.

VeloCloud Gateway

The impact of this CVE on Velocloud Gateway (VCG) is limited due to the following reasons:

- Inbound management services are limited to inbound SSH and are controlled by the operator. Access to Cloud Gateways is highly restricted. Partners are advised on deployment to limit SSH access to trusted networks.
- Tunnel traffic is not affected. SD-WAN overlay traffic uses UDP encapsulation and is not processed by Linux.

For Partner operated Gateways it is recommended to permit inbound SSH only from trusted management networks, and allow only the ports documented in the Gateway deployment guide.

Indicators of Compromise

This vulnerability may lead to a kernel panic on the impacted device. This will appear to be a crash followed by a reboot.

Mitigation

EOS

An event-handler can be configured to configure affected interfaces to use a single receive queue. From the CLI:

```
switch(config)# event-handler MgmtIntf1Ch
action bash sudo ip -all netns exec bash -c 'for i in /sys/class/net/ma*; do ethtool
-L "$(basename "$i")" rx 1; ethtool -L "$(basename "$i")" combined 1; done' &> /dev/n
ull
trigger on-boot
```

This command is applied after being set. Affected management interfaces will flap when the action is run, which can result in the session appearing to freeze for several seconds. If the session does not resume after a minute, close the connection and establish a new one.

VeloCloud Orchestrator

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.

Until a fixed VCO release containing the kernel update is installed, configure each externally reachable network interface to use a single receive queue. This directs incoming packet processing through one receive queue while retaining SYN-cookie protection against SYN floods.

Software receive steering (RPS/RFS) is already disabled in the default VCO configuration and requires no additional configuration changes.

1. **Identify the network interface.**
   Run:

```
ip -br addr
ip route show default
```

   Example output:

```
lo        UNKNOWN   127.0.0.1/8 ::1/128
eth0      UP        10.19.192.56/32
docker0   UP        172.17.0.1/16

default via 10.19.192.1 dev eth0
```

   In this example, **eth0** is the interface used by the default route. Replace **eth0** in the following commands with the applicable interface name on your VCO. If multiple interfaces receive external traffic, repeat the procedure for each applicable interface.

2. **Check and record the current channel count.**

```
sudo ethtool -l eth0
```

   Example output:

```
Channel parameters for eth0:
Pre-set maximums:
RX:             n/a
TX:             n/a
Other:          n/a
Combined:       16
Current hardware settings:
```

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.

```
RX:             n/a
TX:             n/a
Other:          n/a
Combined:       16
```

Read the **Combined** value under **Current hardware settings**. In this example, the current count is **16**. Record this value so the original configuration can be restored after installing the fixed release.

If the current value is already **1**, no channel-count change is needed for this interface.

3. **Reduce the combined-channel count to one.**

```
sudo ethtool -L eth0 combined 1
```

The command normally returns to the prompt without displaying output.

4. **Verify the change.**

```
sudo ethtool -l eth0
```

Expected output for the example above:

```
Channel parameters for eth0:
Pre-set maximums:
RX:             n/a
TX:             n/a
Other:          n/a
Combined:       16
Current hardware settings:
RX:             n/a
TX:             n/a
Other:          n/a
Combined:       1
```

Confirm that **Current hardware settings ? Combined** shows **1**. The **Pre-set**

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.

maximums value remains unchanged.

If the command reports an error, or the interface reports separate RX channels instead of combined channels, contact Arista Support for assistance.

Note: This change takes effect immediately but does not persist across reboots. Reapply the mitigation after each reboot until the fixed VCO release is installed and running.

VeloCloud Gateway & VeloCloud Edge

Arista does not recommend mitigations for VeloCloud Edge or Gateway. The published workaround disables TCP SYN cookies. Disabling them would trade a well-understood protection for a mitigation the products do not need in almost all deployments. The rationale for this is listed in the product specific sections of Required Configuration for Exploitation.

WiFi Access Points

No mitigations are available. Please upgrade to a fixed release when possible.

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

Releases will be added here when available.

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 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:

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.

Subscribeto 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.