**Date: November 18, 2025**

| Revision | Date | Changes |
|---|---|---|
| 1.0 | November 18, 2025 | Initial release |

The CVE-ID tracking this issue: CVE-2025-8873
CVSSv3.1 Base Score: 7.5
(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score 8.7
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N)

Common Weakness Enumeration: CWE-1286: Improper Validation of Syntactic Correctness of Input
This vulnerability is being tracked by BUG 1246592

# Description

On affected platforms running Arista EOS with IPsec configured, a specially crafted packet can cause the dataplane to stop processing all IPsec traffic. The control plane may detect this condition, and attempt to reset the IPsec processing pipeline. After reset traffic may not resume being processed. There is no impact to non-IPsec traffic or to IPsec traffic not originating or terminating on the system.

This issue was reported by an Arista customer. Arista is not aware of any malicious uses of this issue in customer networks.

# Vulnerability Assessment

## Affected Software

### EOS Versions

- 4.33.4M and below releases in the 4.33.x train
- 4.32.6.1M and below releases in the 4.32.x train
- 4.31.7.1M and below releases in the 4.31.x train
- 4.30.10M and below releases in the 4.30.x train
- 4.29.10.1M and below releases in the 4.29.x train

## Affected Platforms

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

- Arista EOS-based products:

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.

    - 7020SRG Series

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

- Arista EOS-based products:
    - 710/710X Series
    - 720D Series
    - 720XP/722XPM Series
    - 750X Series
    - 7010 Series
    - 7010X Series
    - 7020R Series except the 7020SRG
    - 7130 Series running EOS
    - 7150 Series
    - 7160 Series
    - 7170 Series
    - 7050X/X2/X3/X4 Series
    - 7060X/X2/X4/X5/X6 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3/R4 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7800R3/R4 Series
    - 7700R4 Series
    - AWE 5000 Series
    - AWE 7200R Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- CloudVision AGNI
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)

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 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-2025-8873, the following condition must be met:

IPsec must be configured:

```
switch>show ip security connection
Legend: (P) policy based VPN tunnel
Tunnel           Source           Dest             Status       Uptime     Input
       Output           Rekey Time
Tunnel8          10.0.0.1         10.0.0.2         Established  1 minute   0 bytes
       0 bytes          54 minutes
                                                                          30 pkts
       30 pkts
```

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

```
switch>show ip security connection
Legend: (P) policy based VPN tunnel
```

## Indicators of Compromise

This vulnerability may lead to the dataplane ceasing processing of IPsec traffic. When this happens, the following message may appear in “**show logging**”:

```
Jan 1 11:00:00 switch EventMgr: %SYS-4-EVENT_ACTION_LOG: VoqDeleteEventHandler(IpsecF
ap0) triggered 3 times in the last 900 seconds
```

## Mitigation

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.

There are no mitigations for this vulnerability.

## 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-2025-8873 has been fixed in the following releases:

- 4.33.5M and later releases in the 4.33.x train
- 4.32.7M and later releases in the 4.32.x train

After upgrading to a remediated version of software, the system TCAM profile must be changed to ipsec-egress-padding-removal: https://www.arista.com/en/support/toi/tcam-profile?pn=ipsec-egress-padding-removal.

This may momentarily impact traffic. Apply the configuration found at the url to create a TCAM profile and then apply the TCAM profile as shown below.

```
switch(config)#hardware tcam
switch(config-tcam)#system profile ipsec-egress-padding-removal
!
WARNING!
Changing TCAM profile will cause forwarding agent(s) to exit and restart.
All traffic through the forwarding chip managed by the restarting
forwarding agent will be dropped.

Proceed [y/n]y
switch(config-tcam)#
```

To ensure the TCAM profile has been applied, run the following command and verify the Configuration and Status values match **ipsec-egress-padding-removal**:

```
switch(config-tcam)#show hardware tcam profile
                     Configuration             Status
FixedSystem          ipsec-egress-padding-removal
ipsec-egress-padding-removal
```

‘**ipsec-egress-padding-removal**’ differs from the ‘**ipsec**’ TCAM profile in two ways:

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.

- Egress IP ACLs are disabled
- Fixes for BUG603398 and BUG1246592 are applied

## For More Information

If you require further assistance, or if you have any further questions regarding this security advisory, please contact the Arista Networks Technical Assistance Center (TAC) by one of the following methods:

## Open a Service Request

Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support

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.