Date: February 17, 2026

Revision	Date	Changes
1.0	February 17, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-2379
CVSSv3.1 Base Score: 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
Common Weakness Enumeration: CWE-672: Operation on a Resource after Expiration or Release
This vulnerability is being tracked by BUG 1188976

Description

On affected platforms with hardware IPSec support running Arista EOS with certain IPsec features enabled, EOS may exhibit unexpected behavior in specific cases. Physical interface flaps and certain agent restarts can cause IPsec tunnel re-establishment with existing Security Associations, resulting in sequence number mismatches between tunnel endpoints potentially causing unstable communication.

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

Vulnerability Assessment

Affected Software

EOS Versions

- 4.34.3M and below releases in the 4.34.x train
- 4.33.5M and below releases in the 4.33.x train
- 4.32.7M and below releases in the 4.32.x train
- 4.31.9M and below releases in the 4.31.x train
- 4.30.0F and above releases in the 4.30.x train
- 4.29.0F and above releases in the 4.29.x train
- 4.28.0F and above releases in the 4.28.x train
- 4.27.1F and above releases in the 4.27.x train

Affected Platforms

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

- Arista EOS-based products:
  - 7280R3 Series with IPsec:

        - DCS-7280SR3AK, DCS-7280SR3AM
        - DCS-7280CR3AK, DCS-7280CR3AM, DCS-7280CR3MK
        - DCS-7280DR3AK, DCS-7280DR3AM
        - DCS-7289R3AK-SC, DCS-7289R3AM-SC
    - 7800R3 Series with IPsec:
        - 7800R3A-36DM-LC, 7800R3AK-36DM-LC, 7800R3A-36PM-LC, 7800R3AK-36PM-LC, 7800R3A-36DM2-LC, 7800R3AK-36DM2-LC
    - AWE 7000 Series with IPsec:
        - AWE-7250R-16S-F
        - AWE-7230R-4TX-4S-F
        - AWE-7220RP-5TH-2S-F
    - AWE 5000 Series with IPsec:
        - AWE-5510
        - AWE-5310
    - CloudEOS VM

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

- Arista EOS-based products:
    - 710 Series
    - 720D Series
    - 720XP/722XPM Series
    - 750X Series
    - 7010 Series
    - 7010X Series
    - 7020R Series
    - 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 Series
    - 7280R3 and 7280R3A series not listed above, that do not support IPSec
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7800R3 and 7800R3A series not listed above, that do not support IPSec
    - 7800R4 Series
    - 7700R4 Series
    - 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)
- 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-2026-2379, the IPsec **anti-replay detection** feature must be disabled. The IPsec anti-replay detection feature is enabled by default when IPsec is enabled in Arista EOS.

The field “**Replay window size**” in the output of the command “**show ip sec connection detail** ” can be used to verify whether anti-replay is enabled or disabled. A non-zero replay window size indicates that anti-replay detection is enabled.

```
switch#show ip sec connection detail
Tunnel0:
  Source address: 2.0.0.1, Destination address: 2.0.0.2
  State: established
  Uptime: 31 minutes, 49 seconds
  VRF: default
  Inbound SPI: 0xcc09b0d4:
    Request ID: 312, Mode: tunnel, Replay window size: 16384, Seq: 0x0
    Errors:
      Packets outside replay window: 0, Replay: 0, Integrity failed: 0
    Lifetime config:
      Soft byte limit: 3728539143000, Hard byte limit: 6442450944000
      Soft packet limit: 2101671584, Hard packet limit: 4000000000
      Soft time limit: 2657 secs, Hard time limit: 3600 secs
    Lifetime current:
      Current bytes: 461294305
```

```
    Current packets: 391481
    SA add time: Mon Jul  8 00:49:52 2024
    SA last use time: Mon Jul  8 01:21:34 2024
Outbound SPI: 0xc7869a84:
  Request ID: 312, Mode: tunnel, Replay window size: 0, Seq: 0x0
  Errors:
    Packets outside replay window: 0, Replay: 0, Integrity failed: 0
  Lifetime config:
    Soft byte limit: 3616989511500, Hard byte limit: 6442450944000
    Soft packet limit: 2653085513, Hard packet limit: 4000000000
    Soft time limit: 2565 secs, Hard time limit: 3600 secs
  Lifetime current:
    Current bytes: 1421924689
    Current packets: 1207796
    SA add time: Mon Jul  8 00:49:52 2024
    SA last use time: Mon Jul  8 01:21:34 2024
```

In the example above, the replay window size is non-zero which indicates that anti-replay detection is enabled.

If anti-replay detection is enabled, then the vulnerability is not present. The IPsec anti-replay detection feature is disabled with the following configuration:

```
switch(config)# ip security
switch(config-ipsec)# sa policy sa1
switch(config-ipsec-sa1)# no anti-replay detection
```

Indicators of Compromise

No practical ways exist to determine if the system has been compromised.

Mitigation

There is no known mitigation for CVE-2026-2379. The recommended resolution is to upgrade to a remediated software version at your earliest convenience.

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-2026-2379 has been fixed in the following releases:

- 4.35.0F and later releases in the 4.35.x train
- 4.34.4M and later releases in the 4.34.x train
- 4.33.6M and later releases in the 4.33.x train
- 4.32.8M and later releases in the 4.32.x train
- 4.31.10M and later releases in the 4.31.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 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