Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-120974
CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L)
CVSSv4.0 Base Score: 6.9
(CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:H/SA:L)
Common Weakness Enumeration: CWE-294: Authentication Bypass by Capture-replay
This vulnerability is being tracked by BUG 1570728

Description

On affected platforms running Arista EOS with IPsec AutoVPN Feature configured with dynamic paths, the configured IPsec replay window may not be applied as expected. As a result, IPsec anti-replay protection may be silently inactive even when it has been configured via an SA policy, contrary to the operator's expectation. This issue does not allow decryption of the affected IPsec traffic, but it may allow replay of previously valid protected traffic.

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

- 4.36.1F and below releases in the 4.36.x train
- 4.35.5M and below releases in the 4.35.x train
- 4.34.7M 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 4.31.x train
- All releases in the End of Support 4.30.x train
- All releases in the End of Support 4.29.x train
- 4.28.13M and below releases in the 4.28.x train
- All releases in the End of Support 4.27.x train

Affected Platforms

The following products **are** 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:
  - AWE 5000 Series
  - AWE 7200R Series
  - CloudEOS

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/XE7 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
  - 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 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

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)
- 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-2026-120974, the following condition must be met:

Both IPsec AutoVPN Feature and anti-replay window must be enabled:

```
switch> show running-config all section key controller
ip security
   key controller
      profile dp
      dh-group 16
      lifetime 1 hours

switch> show running-config all section anti-replay
ip security
   sa policy dynamic-sa
      anti-replay detection

switch> show ip security key controller local
DH group: 16
Crypto suite: 128-bit AES , 256bit Hash
Initial DH key created: 22 hours, 46 minutes, 43 seconds
Last DH key created: 9 hours, 29 minutes, 40 seconds
DH rekey: N/A
```

If IPsec AutoVPN Feature is not configured or anti-replay window detection is disabled there is no exposure to this issue:

```
switch> show running-config all section key controller

switch> show running-config all section anti-replay
ip security
   sa policy dynamic-sa
      no anti-replay detection
```

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.

Indicators of Compromise

There are no known indicators of compromise for this vulnerability.

Mitigation

There is no known mitigation for CVE-2026-120974. 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-2026-120974 has been fixed in the following releases:

- 4.37.0F and later releases in the 4.37.x train
- 4.36.2F and later releases in the 4.36.x train
- 4.35.6M and later releases in the 4.35.x train
- 4.34.8M and later releases in the 4.34.x train
- 4.33.9M and later releases in the 4.33.x train
- 4.28.14M and later releases in the 4.28.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
- 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.