Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-120975
CVSSv3.1 Base Score: 3.1 (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:L)
CVSSv4.0 Base Score: 2.0
(CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:P/VC:N/VI:L/VA:L/SC:N/SI:L/SA:L)
Common Weakness Enumeration: CWE-197: Numeric Truncation Error
This vulnerability is being tracked by BUG 2047420

Description

On affected platforms running Arista EOS with automatic certificate management configured and automatic Certificate Authority (CA) certificate retrieval enabled, a malicious packet may cause the AutoCertMgmt process to be terminated unexpectedly. Managed X.509 certificates will not be renewed automatically and may eventually expire, potentially disrupting TLS-dependent services.

This issue was discovered internally by Arista, 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

- 4.36.1F release in the 4.36.x train

Affected Platforms

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

- Arista EOS-based products:
  - 710 Series
  - 720D Series

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.

- 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 Serie
- 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

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

- Wi-Fi Access Points
- CloudVision CUE cloud service delivery
- CloudVision Portal, 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)

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 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-2026-120975, the following condition must be met:

Automatic certificate management must be configured with automatic CA certificate retrieval enabled:

```
#show running-config section auto-certificate
management security
   auto-certificate profile cert1
      key clientkey.pem
      parameters distinguished-name common-name "arista"
      protocol instance est1
   auto-certificate protocol est est1
      server url https://example.com
      server ca-certificate auto-update
      server ca-certificate validation fingerprint sha2-256 <...>
```

If automatic certificate management is not configured or if automatic CA certificate retrieval is not enabled, there is no exposure to the issue and the output will either be empty or contain SSL profile usage instead:

```
#show running-config section auto-certificate
management security
   auto-certificate profile cert1
      key clientkey.pem
      parameters distinguished-name common-name "arista"
      protocol instance est1
   auto-certificate protocol est est1
      server url https://example.com
      server ssl profile ssl1
```

Indicators of Compromise

While there are no reliable indicators of compromise for this vulnerability, an unexpected AutoCertMgmt agent crash and restart may be an indication of the issue.

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.

Mitigation

The workaround for the issue is to disable automatic CA certificate retrieval under the auto-certificate protocol and instead use manually distributed CA certificates under an SSL profile. The following CLI commands will disable CA auto update to ensure that data for the certificate retrieval will only come from trusted servers:

```
(config-mgmt-sec-auto-cert-proto-est-est1)# no server ca-certificate auto-update
(config-mgmt-sec-auto-cert-proto-est-est1)# server url https://example.com
(config-mgmt-sec-auto-cert-proto-est-est1)# server ssl profile ssl1
```

For more information about configuring automatic certificate management see EOS User Manual: Automatic Certificate Management.

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-2026-120975 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

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.