Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

Description

These vulnerabilities affect EOS's Resource Public Key Infrastructure (RPKI) client, which obtains Route Origin Authorization(ROA) data from an external cache for Border Gateway Protocol (BGP) route validation. An attacker controlling the RPKI cache or router to cache traffic can send a crafted RPKI message that can cause incorrect validation results or reset the RPKI agent.

These issues were discovered internally by Arista, and the company is not aware of any malicious exploitation of these vulnerabilities in customer networks.

CVE-2026-121291

A crafted Error Report can leave EOS stuck believing that a cache reset is in progress, preventing ROA publication, withdrawal reconciliation, and BGP origin-validation updates.
CVSSv3.1 Base Score: 8.2 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L)
CVSSv4.0 Base Score: 8.3
(CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:L/SC:N/SI:L/SA:N)
Common Weakness Enumeration: CWE-696 Incorrect Behavior Order
This vulnerability is being tracked by BUG 1936844

CVE-2026-121292

A malformed Error Report can cause EOS to read beyond packet boundaries, potentially terminating the RPKI agent or exposing unintended memory contents through logging.
CVSSv3.1 Base Score: 8.2 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H)
CVSSv4.0 Base Score: 8.3
(CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:H/SC:N/SI:L/SA:N)
Common Weakness Enumeration: CWE-125 Out-of-bounds Read
This vulnerability is being tracked by BUG 1936846.

Vulnerability Assessment

Platform and Software Applicability Note

To determine actual exposure, operators should first check their EOS version against the affected ranges below and verify whether RPKI cache connectivity is configured. If RPKI is not configured, these issues cannot be reached through the RPKI protocol.

Affected Software

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.

EOS Versions

CVE-2026-121291:

- 4.37.0F
- 4.36.2F and below releases in the 4.36.x train
- 4.35.6M and below releases in the 4.35.x train

Releases before 4.35.0F are not affected.

CVE-2026-121292:

- 4.37.0F
- 4.36.2F and below releases in the 4.36.x train
- 4.35.6M and below releases in the 4.35.x train
- 4.34.8M and below releases in the 4.34.x train
- 4.33.10M and below releases in the 4.33.x train
- All releases in the End of Support software release trains, beginning with 4.24.0F

Releases before 4.24.0F are not affected.

Affected Platforms

The following products **are** affected by CVE-2026-121291 and CVE-2026-121292:

- 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

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.

  - 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 on-premises, 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)
- 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)
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision Portal, virtual appliance or physical appliance

Required Configuration for Exploitation

CVE-2026-121291 and CVE-2026-121292

To be vulnerable to either vulnerability, an EOS device must have one or more RPKI caches configured and establish an RPKI-to-Router (RPKI-RTR) session. Operators can verify this with:

```
switch> show bgp rpki cache
```

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.

The configuration should contain an RPKI cache entry under BGP, for example:

```
router bgp <ASN>
     rpki cache <cache-name>
        host <cache-address>
```

Indicators of Compromise

CVE-2026-121291

This vulnerability may leave RPKI reset synchronization incomplete, preventing ROA updates and withdrawals from being published to BGP origin validation.

1. Check the logs for RPKI synchronization errors

   An Error Report received during reset synchronization may appear in show logging:

   ```
   Jan 1 00:00:41 switch %R
   PKI-4-CACHE_ERROR: Received 1:Internal Error
    from cache server 192.0.2.10 ('cache1')
   Jan 1 00:00:42 switch %R
   PKI-4-CACHE_ERROR: Received 2:No Data Available
    from cache server 192.0.2.10 ('cache1')
   ```

   These messages can be found with the following grep commands from the bash shell:

   ```
   grep "RPKI-4-CACHE_ERROR: Received" /var/log/eos
   ```

2. Check the RPKI error counters

   ```
   switch>enable
   switch#show bgp rpki cache cache1 counters errors
   ```

   Review Internal Error, No Data, and Corrupt Data, comparing them with previously recorded values.

3. Check whether synchronization recovered

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.

```
switch#show bgp rpki cache cache1
```

Correlate the increased error counters with a cache showing awaiting ROA data or disabled, or whose Last full sync timestamp does not advance.

CVE-2026-121292

The vulnerability may cause the RPKI agent to terminate or restart after receiving an RPKI malformed message.

The following message may appear in show logging:

```
Jan 1 00:00:41 switch %RPKI-4-CACHE_ERROR:
 Received malformed Error Report PDU from cache server 192.0.2.10 ('cache1')
```

The malformed-PDU message can be found with the following grep command from the bash shell:

```
grep "Received malformed Error Report PDU from cache server" /var/log/eos
```

Operators should preserve relevant RPKI and system logs and review the configured cache and transport when investigating these symptoms.

Mitigation

CVE-2026-121291 and CVE-2026-121292

No mitigation is available for these vulnerabilities. Customers should upgrade to a remediated EOS release as soon as possible. For CVE-2026-121291, clearing the affected RPKI cache using clear bgp rpki cache <cache-name> or restarting the RPKI agent may recover from a stuck synchronization state, but does not prevent recurrence.

Resolution

The recommended resolution is to upgrade to a remediated software version at the earliest opportunity. Arista recommends customers move to the latest release in each train that contains all applicable fixes. For more information about upgrading, see the EOS User Manual: Upgrades and Downgrades.

CVE-2026-121291 has been fixed in:

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.

- 4.36.3M and later releases in the 4.36.x train
- 4.35.7M and later releases in the 4.35.x train

CVE-2026-121292 has been fixed in:

- 4.36.3M and later releases in the 4.36.x train
- 4.35.7M and later releases in the 4.35.x train
- 4.34.9M and later releases in the 4.34.x train
- 4.33.11M and later releases in the 4.33.x train

Hotfix

CVE-2026-121291 and CVE-2026-121292

No hotfix is available for these issues.

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.