Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release — draft for review

The CVE-ID tracking this issue: CVE-2026-121367
CVSSv3.1 Base Score: 9.6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:H)
CVSSv4.0 Base Score: 6.1
(CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:L/SA:L)
Common Weakness Enumeration: CWE-440: Expected Behavior Violation
This vulnerability is being tracked by BUG 1981966

Description

On affected Arista EOS platforms with Routing Information Protocol version 2 (RIPv2) configured, under certain conditions, RIPv2 might be silently enabled on management interfaces even when the RIP agent intends to disable it. It allows an unauthenticated attacker with access to the adjacent network to send crafted RIPv2 route advertisements to the device's management IP address. The device could accept and install those routes without authentication.

Successful exploitation could allow the attacker to redirect traffic flows to an attacker-controlled destination, install more-specific routes that blackhole legitimate traffic, or otherwise disrupt network reachability for systems whose traffic passes through the affected device.

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

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

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.

- 4.34.8M 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 4.32.x train
- All releases in the End of Support software release trains

Affected Platforms

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

- 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
  - 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

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.

- 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)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2026-121367, the following conditions must both be met:

- RIP is enabled
- RIP network configuration matches the subnet assigned to the management interface in the same VRF

RIP processing on the management interface may not appear in running configuration, so routine configuration review may not reveal the exposure.

```
switch# show running-config section router rip
router rip
   network 10.252.36.128/25
   no shutdown

switch# show running-config section interface Management1
interface Management1
   ip address 10.252.36.194/25
```

Indicators of Compromise

While there are no direct indicators of compromise, unexpected RIP-learned routes, unapproved next hops, more-specific routes, or route changes that redirect traffic or disrupt reachability may indicate unauthorized RIP advertisements.

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.

Compare current routes with the approved routing design and known peer inventory with the following command:

```
switch# show ip route
```

Mitigation

In environments where RIP is not required, it should be disabled within each affected VRF instance. Please note that disabling RIP or changing network statements may withdraw routes and interrupt connectivity. Plan a change window, confirm alternate routing, and verify the resulting configuration and route behavior.

The following example disables the default-VRF RIP instance:

```
switch# configure terminal
switch(config)# router rip
switch(config-router-rip)# shutdown
switch(config-router-rip)# end
```

If RIP is necessary on data interfaces but not on the management subnet, verify that no RIP network prefix matches that management subnet. The specific configuration details are delineated in the above Required Configuration for Exploitation section.

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-2026-121367 has been fixed in the following releases:

- 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

No hotfix is available for this 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.

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.