Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

Description

This advisory covers two vulnerabilities in the Routing Information Protocol version 2 (RIPv2) MD5 authentication on Arista EOS-based products. An unauthenticated attacker with adjacent network access may be able to interrupt routing services or inject unauthorized routes.

CVE-2026-121287

An unauthenticated attacker on an adjacent network segment can send crafted RIPv2 packets to a RIP-enabled interface on the device to trigger the Rip agent crash without providing valid credentials. Repeated exploitation reliably interrupts routing service on the affected device, which may also disrupt routing for other devices that depend on it. In a worst-case scenario, the vulnerability may allow an attacker to execute arbitrary code on the affected device.

CVSSv3.1 Base Score: 8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSSv4.0 Base Score: 7.7
(CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:L/SA:N)
Common Weakness Enumeration: CWE-124 Buffer Underwrite ('Buffer Underflow')
This vulnerability is being tracked by BUG 1981970

This issue was discovered internally by Arista, and the company is not aware of any malicious exploitation of this vulnerability in customer networks.

CVE-2026-121288

An unauthenticated attacker on an adjacent network segment can bypass MD5 authentication and have unauthorized RIP route updates accepted by the device. Successful exploitation requires that RIPv2 MD5 authentication is configured on the affected interface. An attacker who can inject crafted RIPv2 packets could cause the device to install routes that redirect network traffic through attacker-controlled paths, create routing loops, or blackhole traffic, disrupting network connectivity.

CVSSv3.1 Base Score: 8.1 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)
CVSSv4.0 Base Score: 6.1
(CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:H/SC:N/SI:L/SA:L)
Common Weakness Enumeration: CWE-303 Incorrect Implementation of Authentication Algorithm
This vulnerability is being tracked by BUG 1985547

Arista would like to acknowledge and thank Joshua Foote from the XOR team at JP Morgan

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.

Chase for responsibly reporting CVE-2026-121288.

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

CVE-2026-121287 and CVE-2026-121288

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
- 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

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.

  - 7388X5 Series
  - 7500R/R2/R3 Series
  - 7800R3/R4 Series
  - 7700R4 Series
  - AWE 5000 Series
  - AWE 7200R 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 Portal, virtual appliance or physical appliance
- 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)

Required Configuration for Exploitation

CVE-2026-121287 and CVE-2026-121288

In order to be vulnerable to CVE-2026-121287 and CVE-2026-121288, the following three conditions must be met:

- RIP is enabled

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.

- MD5 authentication configured on an interface
- RIP network configuration must match the interface ip-address

```
switch# show running-config | section router rip
router rip
   no shutdown
   network 192.0.2.0/24

switch# show running-config interfaces Ethernet1
interface Ethernet1
   ip address 192.0.2.1/24
   rip authentication algorithm md5 tx key-id 10
```

Indicators of Compromise

CVE-2026-121287

While there are no direct indicators of compromise, unexpected Rip agent termination or repeated restarts may serve as potential warning signs of the issue.

Check logs for Rip-related events and correlate their timestamps with the routing disruption with the following command:

```
switch# show logging | include Rip
ProcMgr-worker: %PROCMGR-6-PROCESS_TERMINATED: 'Rip' (PID=<old-pid>) has terminated.
ProcMgr-worker: %PROCMGR-6-PROCESS_RESTART: Restarting 'Rip' immediately (it had PID=
<old-pid>)
ProcMgr-worker: %PROCMGR-6-PROCESS_STARTED: 'Rip' starting with PID=<new-
pid> (PPID=<parent-pid>) -- execing '/usr/bin/Rip'
```

CVE-2026-121288

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.

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

```
switch# show ip route
```

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

CVE-2026-121287 and CVE-2026-121288

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

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

All of the CVEs have 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 to mitigate the issues listed in the advisory.

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

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.

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.