Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release
1.1	September 22, 2026	CSAF JSON file added

Description

All of the CVEs covered in this advisory apply to affected platforms running Arista EOS with the Virtual Router Redundancy Protocol (VRRP) enabled.

In addition, CVE-2026-73444 and CVE-2026-73443 require version 2 (VRRPv2) configured with VRRPv2 authentication enabled. VRRPv2 is the default version for Arista EOS but VRRP Authentication is not enabled by default. VRRP version 3 (VRRPv3) and VRRPv2 deployments without authentication are not affected by those two issues.

Note: While Arista EOS supports VRRPv2 authentication, it is a deprecated mechanism in the standards: VRRPv2 was defined in RFC 2338 and removed from the VRRP specification in RFC 3768, and the text authentication mode transmits the password in cleartext on the local network segment by design. It is recommended to use VRRPv3 instead.

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

CVE-2026-73444

On affected platforms running Arista EOS with VRRPv2 IP Authentication Header (IP-AH) authentication configured, an unauthenticated attacker with access to the layer 2 network segment on which VRRP is running could bypass VRRP authentication and claim the virtual router master role, enabling the attacker to intercept, modify, or discard traffic that hosts on the segment send to the virtual gateway address.

CVSSv3.1 Base Score: 4.7 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L)
CVSSv4.0 Base Score: 5.3
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-303 Incorrect Implementation of Authentication Algorithm
This vulnerability is being tracked by BUG 1866656

CVE-2026-73443

On affected platforms running Arista EOS with VRRPv2 IP-AH authentication configured, an unauthenticated attacker within the same layer 2 network segment on which VRRP is running can capture a legitimate authenticated VRRP advertisement and replay it indefinitely. Replayed

advertisements can be used to advertise stale VRRP state, for example to prevent a backup router from taking over the virtual gateway after the original master has gone down, resulting in a denial of service for hosts using the virtual gateway address.

CVSSv3.1 Base Score: 4.7 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L)
CVSSv4.0 Base Score: 5.3
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-294 Authentication Bypass by Capture-replay
This vulnerability is being tracked by BUG 1866651

CVE-2026-73442

On affected platforms running Arista EOS with VRRP enabled, the peer device VRRP authentication credentials are logged in cleartext on the switch, allowing an authenticated user with sufficient privileges to view agent trace logs (or a system receiving forwarded log output) to obtain the peer device VRRP authentication credentials without having access to the network segment on which VRRP is running.

CVSSv3.1 Base Score: 3.0 (CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:C/C:L/I:N/A:N)
CVSSv4.0 Base Score: 2.1
(CVSS:4.0/AV:A/AC:H/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N)
Common Weakness Enumeration: CWE-532 Insertion of Sensitive Information into Log File
This vulnerability is being tracked by BUG 1857627

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 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
- 4.33.9M and below releases in the 4.33.x train
- All prior releases

Affected Platforms

The following products **are** affected by these vulnerabilities:

- 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 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
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance

The following product versions and platforms **are not** affected by these vulnerabilities:

- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- 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 7130 Systems running MOS
- 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-2026-73444 and CVE-2026-73443

In order to be vulnerable to CVE-2026-73444 or CVE-2026-73443, the following condition must be met:

VRRPv2 must be configured with IP-AH authentication on at least one interface (a vulnerable configuration shows a virtual router with version 2 (the default version) and IP-AH authentication):

```
switch>show running-config section vrrp
interface Ethernet1
   vrrp 1 ipv4 version 2
   vrrp 1 peer authentication ietf-md5 key-string 7 <key>
```

If VRRP is not configured, or is configured as version 3, or is configured without authentication, there is no exposure to the above two CVEs.

CVE-2026-73442

In order to be vulnerable to CVE-2026-73442, the following condition must be met:

1. VRRP must be configured

```
switch>show running-config section vrrp
interface Ethernet1
   vrrp 1 ipv4 <ipAddr>
```

If VRRP is not configured, there is no exposure to CVE-2026-73442.

Indicators of Compromise

There are no indicators of compromise for these CVEs.

Mitigation

CVE-2026-73444 and CVE-2026-73443

Exposure is limited to attackers with access to the layer 2 network segment on which VRRP is running. Restricting physical and logical access to VRRP-enabled segments (for example with port security and by not extending VRRP VLANs to untrusted access ports) reduces the attack surface. Additionally, migrating virtual routers from VRRP version 2 with authentication to VRRP version 3 removes the vulnerable code path.

The below configuration shows how to configure VRRPv3 on VLAN 20:

```
switch(config)# interface vlan 20
switch(config-if-vl20)# vrrp 1 ipv4 version 3
```

CVE-2026-73442

If the VRRP feature is not operationally required, disabling it removes the exposure. Otherwise, there is no mitigation or workaround available. Please note that disabling VRRP can lead to network outages if the primary router fails.

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-2026-73444, CVE-2026-73443, and CVE-2026-73442 have been fixed in the following releases:

- 4.36.2F and above releases in the 4.36.x train
- 4.35.6M and above releases in the 4.35.x train
- 4.34.8M and above releases in the 4.34.x train
- 4.33.10M and above releases in the 4.33.x train

Important: For CVE-2026-73443, upgrading alone is not sufficient. The replay protection introduced by the fix is disabled by default and must be explicitly enabled with the following new global configuration command after upgrading to a remediated release:

```
switch(config)#vrrp ipv4 authentication anti-replay
```

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

Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support