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

The CVE-ID tracking this issue: CVE-2026-19655
CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 7.1
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-20 Improper Input Validation
This vulnerability is being tracked by BUG 1770194

Description

On affected platforms running Arista EOS with Dynamic Host Configuration Protocol (DHCP) relay/snooping configured with the information option (Option 82), or with the DHCP server configured with match criteria based on the information option, an unauthenticated attacker connected to a client-facing VLAN(s) where the relay is configured can send a specially crafted packet that causes the DHCP Relay service to restart.

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

- 4.35.5M and below releases in the 4.35.x train
- 4.34.7.1M 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 this vulnerability:

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 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 this vulnerability:

- Wi-Fi 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

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.

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-2026-19655, any of the following conditions must be met:

Configure "**ip dhcp relay**" with the "**information option**" (Option 82) and at least one helper-address on an interface:

```
interface Vlan100
   ip helper-address 1.1.1.2
ip dhcp relay information option
```

Or

Configure "**ip dhcp snooping**" with the "**information option**":

```
switch#show running-config | grep snooping
ip dhcp snooping
ip dhcp snooping information option
ip dhcp snooping vlan 100
```

Or

The DHCP server uses match criteria based on the information option, configured with "**information option arista-switch**" commands. Below is an example of configuring the DHCP server to match requests containing Arista switch information that identifies Ethernet55/1 and VLAN 100 in DHCP Option 82.:

```
dhcp server
   client class ipv4 definition name
      assignments
         private-option 224 always-send type string data ""data1""
      !
      match
         information option arista-switch Ethernet55/1 vlan 100
```

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.

```
   !
   subnet 1.0.0.0/24
      range 1.0.0.1 1.0.0.5
interface Vlan10
   dhcp server ipv4
```

Indicators of Compromise

This vulnerability may lead to DhcpRelay agent restarting; an example of such a restart is included here.

```
Apr 27 03:30:59 switch ProcMgr-
worker: %PROCMG
R-6-PROCESS_RESTART: Restarting 'DhcpRelay' immediately (it had PID=4107)
Apr 27 03:30:59 switch ProcMgr-worker: %PROCMGR-7-PREDECESSOR_WAITING: New instance o
f DhcpRelay (PID=5103): waiting for reaping of predecessor (PID=4107)
Apr 27 03:30:59 switch ProcMgr-worker: %PROCMGR-7-PREDECESSOR_GONE: New instance of D
hcpRelay (PID=5103): predecessor (PID=4107) has been reaped.
Apr 27 03:30:59 switch ProcMgr-worker: %PROCMGR-6-PROCESS_STARTED: 'DhcpRelay' starti
ng with PID=5103 (PPID=1949) -- execing '/usr/bin/DhcpRelay'
Apr 27 03:30:59 switch DhcpRelay: %AGENT-6-INITIALIZED: Agent 'DhcpRelay' initialized
; pid=5103
```

These messages can be found in the EOS CLI through the “**show logging**”. If in privileged mode or higher the “**show logging**” output can be piped to the following grep commands in the EOS Cli.

```
switch# show logging | grep "PROCMGR-6-PROCESS_RESTART.*DhcpRelay"
switch# show logging | grep "PROCMGR-7-PREDECESSOR_WAITING.*DhcpRelay"
switch# show logging | grep "PROCMGR-7-PREDECESSOR_GONE.*DhcpRelay"
switch# show logging | grep "PROCMGR-6-PROCESS_STARTED.*DhcpRelay"
switch# show logging | grep "AGENT-6-INITIALIZED.*DhcpRelay"
```

Mitigation

There is no workaround known for this issue.

Resolution

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 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-2026-19655 has been fixed in the following releases:

- 4.35.6M and later releases in the 4.35.x train
- 4.34.8M and later releases in the 4.34.x train
- 4.33.10M and later releases in the 4.33.x train

Hotfix

No hotfix is available to remediate CVE-2026-19655.

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

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.