Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-73437
CVSSv3.1 Base Score: 9.6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
CVSSv4.0 Base Score: 6.5
(CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:H/SI:H/SA:H)
Common Weakness Enumeration: CWE-345 Insufficient Verification of Data Authenticity
This vulnerability is being tracked by BUG 1869660

Note: CVSS v3.1 captures impact on the secondary system through Scope:Changed, combining direct and downstream impact (confidentiality, integrity and availability) using the impact metrics, which often inflates the overall severity. CVSS v4.0 separates the vulnerable component from the subsequent system, allowing the limited direct impact and the higher downstream impact to be scored independently; this distinction can produce a significantly lower v4.0 score.

Description

On affected platforms running Arista EOS with Dynamic Host Configuration Protocol (DHCP) relay configured, an unauthenticated attacker with network access could send a crafted DHCP reply packet from an IP address that is not configured as a helper/destination address, and the relay agent would forward it to clients without validating the source. This could allow the attacker to supply clients with malicious network configuration parameters, potentially resulting in traffic interception or denial of service for affected clients.

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 and the DHCP packet strict validation is configured as instructed in the Resolution section, 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
- 4.34.7.1M 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:

- 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 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

To be vulnerable to CVE-2026-73437, the DHCP relay must be configured, and either an IPv4 or IPv6 helper address must be configured for the DHCP relay to be active.

E.g., Configuring an IPv4 helper address

```
switch# configure terminal
switch(config)#int vlan 100
switch(config-if-Vl100)#ip helper-address 10.40.2.3
```

E.g., Configuring an IPv6 helper address

```
switch# configure terminal
switch(config)#int vlan 100
switch(config-if-Vl100)#ipv6 helper-address 3ffe:701:ffff:100::2
```

The above config can be validated as mentioned below:

```
switch>show ip dhcp relay
DHCP relay is active
...
Interface: Vlan100
```

```
DHCPv4 servers: 10.40.2.3
DHCPv6 servers: 3ffe:701:ffff:100::2
```

If DHCP relay is not active (no helper addresses), there is no exposure to this issue:

```
switch>show ip dhcp relay
DHCP relay is not active
```

Indicators of Compromise

An attacker exploiting this vulnerability would send DHCP reply packets (DHCPOFFER, DHCPACK, or DHCPv6 Relay-Reply) from an IP address that is not a configured helper/destination and relay agent forwards them without validating the source.

```
switch>show ip dhcp relay counters

DHCP Packets
Globals   Rcvd Fwdd Drop Last Cleared
--------- ---- ---- ---- ------------
All Req   11   11   0    0:34:55 ago
All Resp  11   11   0

DHCP Request Packets
Interface  Rcvd Fwdd Drop Last Cleared
---------- ---- ---- ---- ------------
Ethernet3  11   11   0    0:09:20 ago
Ethernet5  0    0    0    0:09:19 ago

DHCP Reply Packets
Interface  Rcvd Fwdd Drop Last Cleared
---------- ---- ---- ---- ------------
Ethernet3  0    0    0    0:09:20 ago
Ethernet5  11   11   0    0:09:19 ago
```

There is no indicator before upgrading to a remediated version of EOS. After upgrading and enabling **reply source-address validation** config suggested in the Resolution section, the following message can be found under /var/log/agent/DhcpRelay-*:

```
…reply from server 192.168.1.2 not a configured helper for client interface Ethernet3
. Dropping packet.
```

Also, the following show command output reflects the packet drops after upgrading.

```
switch>show ip dhcp relay counters

DHCP Packets
Globals   Rcvd Fwdd Drop Last Cleared
--------- ---- ---- ---- ------------
All Req   11   11   0    0:34:55 ago
All Resp  11   0    11

DHCP Request Packets
Interface  Rcvd Fwdd Drop Last Cleared
---------- ---- ---- ---- ------------
Ethernet3  11   11   0    0:09:20 ago
Ethernet5  0    0    0    0:09:19 ago

DHCP Reply Packets
Interface  Rcvd Fwdd Drop Last Cleared
---------- ---- ---- ---- ------------
Ethernet3  0    0    0    0:09:20 ago
Ethernet5  11   0    11   0:09:19 ago
```

Mitigation

IP locking can be run in a locked address enforcement disabled state, along with the DHCP Relay, to provide protection against rogue DHCP servers and spoofing. This is supported on DHCPv4 starting with EOS-4.29.0F and on DHCPv6 starting with EOS-4.27.0F. For more information, see IP Locking.

This is compatible with the following platforms only:

- CCS-720XP
- CCS-710P
- CCS-720DP
- CCS-722XPM
- DCS-7010TX
- DCS-7050CX3
- DCS-7050SX3
- CCS-710XP
- CCS-720DF
- CCS-720DT

- CCS-720XDM
- CCS-720XPM
- CCS-755
- CCS-758
- DCS-7050CX3M
- DCS-7050TX3
- DCS-7304
- DCS-7308
- 7300X3

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience and enable the **reply source-address validation** CLI knob under dhcp relay mode.

```
switch(config)# dhcp relay
switch(config-dhcp-relay)# reply source-address validation
```

The knob defaults to disabled for backward compatibility. When enabled, the relay agent validates that the source IP of every DHCP server reply matches a configured helper address (IPv4) or relay destination (IPv6) for the client-facing interface. Replies from unconfigured sources are dropped.

Note that the strict validation against the configured helper address/destination will drop legitimate replies from any server whose source IP doesn't exactly match the configured address. This could break real deployments, such as:

- The server has multiple interfaces
- The server's kernel picks a different source address

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-2026-73437 has been fixed in the following releases:

- 4.36.2F and later releases in the 4.36.x train
- 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

Note: All versions require upgrading to a release containing the fix (as listed above) as we're

not providing any hotfix.

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