Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-73469
CVSSv3.1 Base Score: 5.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N)
CVSSv4.0 Base Score: 6.9
(CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-863: Incorrect Authorization
This vulnerability is being tracked by BUG 1353206

Description

When specific platforms are using Arista EOS with a loose Unicast Reverse Path Forwarding (uRPF) configuration, certain traffic may not be subjected to the intended verification drop. Consequently, traffic that should be dropped based on these routes could still be processed and forwarded by the device.

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

Vulnerability Assessment

Affected Software

EOS Versions

- 4.35.4M and below releases in the 4.35.x train

Affected Platforms

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

- Arista EOS-based products:
  - 7050X4 Series
  - 7358X4 Series

The following product versions and platforms **are not** affected by this vulnerability:

- Arista EOS-based products:
  - 710 Series

    - 720D Series
    - 720XP/722XPM Series
    - 750X Series
    - 7010 Series
    - 7010X Series
    - 7020R Series
    - 7130 Series running EOS
    - 7150 Series
    - 7160 Series
    - 7170 Series
    - 7050X/X2/X3 Series
    - 7060X/X2/X4/X5/X6 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3/R4 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/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
- 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 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-2026-73469, loose mode uRPF must be configured on an interface. This can be checked by showing the interface status, or by checking the current switch config.

```
switch>show ip interface
Ethernet1/1 is up, line protocol is up (connected)
  Internet address is 192.0.2.1/24
  Broadcast address is 255.255.255.255
  IPv4 interface forwarding: enabled
  IPv6 interface forwarding: none
  IP verify unicast source reachable-via any
  Proxy-ARP is disabled
  Local Proxy-ARP is disabled
  Gratuitous ARP is ignored
  ARP aging timeout is 14400 seconds
  IP MTU 1500 bytes
...

switch>show ipv6 interface

Ethernet1/1 is up, line protocol is up (connected)
  IPv6 is enabled, link-local is fe80::200:5eff:fe00:53fe/64
  Global unicast address(es):
    2001:db8::1, subnet is 2001:db8::/64
  Joined group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:1
    ff02::1:ff00:53fe
  IPv6 verify unicast source reachable-via any
  ND DAD is enabled, number of DAD attempts: 1
  ND Reachable time is 2147483000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND enhanced duplicate address detection enabled
  ND advertised reachable time is 2147483000 milliseconds (using 2147483000)
  ND advertised retransmit interval is 1000 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

```
  ND advertised default router preference is Medium
  ND advertised maximum hop count limit is 64
  Hosts use stateless autoconfig for addresses.
  ND unsolicited NAs are not accepted
  ND cache expiry time is 14400 seconds
...

switch>show running-config section ip verify
interface Ethernet1/1
  ip verify unicast source reachable-via any

switch>show running-config section ipv6 verify
interface Ethernet1/1
  ipv6 verify unicast source reachable-via any
```

If loose mode uRPF is not configured on an interface, there is no exposure to this issue. In this example, Ethernet1/1 is configured with strict mode uRPF, and Ethernet2/1 is not configured with any uRPF. Therefore neither are affected.

```
switch>show ip interface
Ethernet1/1 is up, line protocol is up (connected)
  Internet address is 192.0.2.1/24
  Broadcast address is 255.255.255.255
  IPv4 interface forwarding: enabled
  IPv6 interface forwarding: none
  IP verify unicast source reachable-via RX
  Proxy-ARP is disabled
  Local Proxy-ARP is disabled
  Gratuitous ARP is ignored
  ARP aging timeout is 14400 seconds
  IP MTU 1500 bytes
Ethernet2/1 is up, line protocol is up (connected)
  Internet address is 198.51.100.1/24
  Broadcast address is 255.255.255.255
  IPv4 interface forwarding: enabled
  IPv6 interface forwarding: none
  Proxy-ARP is disabled
  Local Proxy-ARP is disabled
  Gratuitous ARP is ignored
  ARP aging timeout is 14400 seconds
  IP MTU 1500 bytes
```

Indicators of Compromise

No indicators of compromise exist.

Mitigation

No mitigation exists for this issue.

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-2026-73469 has been fixed in the following releases:

- 4.36.0F and later releases in the 4.36.x train
- 4.35.5M and later releases in the 4.35.x train

Hotfix

No hotfix is provided for this issue.

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