Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-73449
CVSSv3.1 Base Score: 5.9 (CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:L)
CVSSv4.0 Base Score: 5.9
(CVSS:4.0/AV:A/AC:L/AT:P/PR:L/UI:N/VC:N/VI:H/VA:N/SC:N/SI:L/SA:L)
Common Weakness Enumeration: CWE-290 (Authentication Bypass by Spoofing)
This vulnerability is being tracked by BUG 1697784.

Description

On affected platforms running Arista EOS with both 802.1X port authentication and the RADIUS proxy feature configured with dynamic authorization, a low-privileged attacker on an adjacent network segment who induces a RADIUS packet through a configured RADIUS proxy client can prevent RADIUS dynamic authorization messages, including Change-of-Authorization (CoA) and Disconnect-Requests as defined in RFC 5176, from being applied to locally authenticated 802.1X sessions.

This allows an endpoint session that a RADIUS server or network access control system has ordered disconnected to remain authorized on the network.

Both 802.1X port authentication with dynamic authorization and RADIUS proxy with dynamic authorization must be explicitly configured for a deployment to be exposed to this issue.

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

- 4.36.1F 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

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

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

- Arista EOS-based products:
  - 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 as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- CloudVision Appliance Software

- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)
- Arista Multi Cloud Director (formerly Big Switch MCD)
- 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 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-2026-73449, both of the following conditions must be met:

1. 802.1X must be enabled with RADIUS dynamic authorization

   The running configuration must contain **dot1x system-auth-control** and **dot1x dynamic-authorization**, with one or more interfaces configured for authentication:

```
switch# show running-config section dot1x
dot1x system-auth-control
dot1x dynamic-authorization
...
interface Ethernet1
   dot1x pae authenticator
   dot1x port-control auto
```

   Authenticated 802.1X sessions can be listed with:

```
switch#show dot1x hosts
Port  Supplicant MAC  Username           Auth State    Fallback  VLAN VLAN Nam
e
----- --------------- ------------------ ---- -------  --------- ---- --------
--
Et30  0017.0100.0001  00:17:01:00:00:01  MBA  SUCCESS  NONE      30*  VLAN0030
Et30  606b.5ba7.73c5  60:6b:5b:a7:73:c5  MBA  SUCCESS  NONE      30*  VLAN0030
```

2. RADIUS proxy must be enabled with dynamic authorization

   The running configuration contains a **radius proxy** section with at least one client group and the **dynamic-authorization** command:

```
switch# show running-config section radius proxy
radius proxy
   dynamic-authorization
   client group CG1
      client ipv4 10.0.0.0/24 vrf default
      server group SG1
```

   The state of the RADIUS proxy feature can be confirmed with:

```
switch# show radius proxy client group
Radius Client Group                    : CG1
Last time counters were cleared        : never
Dynamic authorization                  : enabled
Dynamic authorization destination port : <portNumber>

   Client                          : <clientName>, authentication port 1812, a
ccounting port 1813, vrf default
   Resolved IP address             : <resolvedIp>
…
```

   If the output of this command shows "**Dynamic authorization: disabled**", or if either the **radius proxy** section or the 802.1X configuration above is absent, there is no exposure to the issue.

Indicators of Compromise

The presence of **all** the following indicators on the system confirms that a compromise has occurred:

1. An endpoint continues to be displayed as authenticated within the output of **show dot1x hosts** following the transmission of a Disconnect or Change of Authorization (CoA) request by the authentication server to terminate the associated supplicant session. Please note that this condition alone does not definitively confirm a compromise, as it may occur during standard operational windows. All available indicators should be thoroughly evaluated to establish whether a compromise has occurred.

```
switch#show dot1x hosts
Port  Supplicant MAC  Username           Auth State    Fallback  VLAN VLAN Nam
e
----- -------------- ------------------ ---- -------  --------- ---- --------
--
Et30  0017.0100.0001  00:17:01:00:00:01  MBA  SUCCESS  NONE      30*  VLAN0030
Et30  606b.5ba7.73c5  60:6b:5b:a7:73:c5  MBA  SUCCESS  NONE      30*  VLAN0030
```

2. The authentication server logs may indicate CoA-NAK (Negative AcKnowledgement) or Disconnect-NAK responses, particularly with Error-Cause 503 ('Session Context Not Found'), or missing responses, for sessions that are active on the switch. Please note that as RADIUS server logging formats and interface views are highly vendor-specific, generalized log examples cannot be provided. Administrators should examine their specific server logs to verify these conditions.
3. Anomalous dynamic authorization counters
    - Run the following command to inspect the proxy client group counters:

```
(switch)# show radius proxy client group | grep -E 'CoA|DM'
                  CoA requests sent:          5
                   DM requests sent:          6
                  CoA ACKs received:          0
                   DM ACKs received:          0
                  CoA NAKs received:          0
                   DM NAKs received:          0
```

      Monitor the "CoA requests sent" and "DM requests sent" counters. If these **counters are increasing** when the server sends a CoA or DM (Disconnect Message) request for active Dot1x sessions, it confirms the RADIUS proxy is incorrectly intercepting and rerouting those packets downstream.

    - To check if CoA/DM requests for active Dot1x sessions are being dropped or NAK'd, run **show radius** and verify if the counters balance using this formula:

      CoA/DM Requests Received = CoA/DM ACKs Sent + CoA/DM NAKs Sent

        - Normal Behavior: Every request is processed successfully (Requests Received = ACKs Sent, with NAKs remaining constant).
        - Active Rejection (NAKs): The counters balance, but NAKs Sent are increasing instead of ACKs.
        - Silent Drops: The equation is unequal (Requests Received > ACKs Sent + NAKs Sent). This confirms that incoming requests are increasing with no corresponding ACKs or NAKs, meaning the switch is silently discarding the packets without responding.

```
(switch)#show radius | grep -E 'CoA|DM'
     CoA requests received:          5
      DM requests received:          5
             CoA ACKs sent:          0
              DM ACKs sent:          0
             CoA NAKs sent:          2
              DM NAKs sent:          5
```

Mitigation

If the RADIUS proxy dynamic authorization function is not operationally required, disabling it removes the exposure. Please note this operation will stop the switch from forwarding CoA and Disconnect requests to downstream RADIUS proxy clients. Dynamic authorization of the switch's own local 802.1X sessions continues to work.

```
switch(config)# radius proxy
switch(config-radius-proxy)# no dynamic-authorization
```

If RADIUS proxy dynamic authorization must remain enabled, the exposure window can be reduced (but not eliminated) by lowering the proxy client session idle timeout from its default of 600 seconds:

```
switch(config)# radius proxy
switch(config-radius-proxy)# client session idle-timeout <seconds> seconds
```

Note that if the idle-timeout is being reduced, then radius proxy clients should increase the frequency of interim-update accounting requests. For more information about idle-timeout configuration see “Configuring session idle-timeout” section in RADIUS Proxy.

If a specific endpoint must be forcibly disconnected while this issue is unresolved, the following command can be used.

```
switch(config)# clear dot1x host mac <endpoint macAddress>
```

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-2026-73449 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

Hotfix

No hotfix is available 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