Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release

The CVE-ID tracking this issue: CVE-2026-120977
CVSSv3.1 Base Score: 8.2 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:L/I:H/A:N)
CVSSv4.0 Base Score: 7.1
(CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:L/SI:H/SA:N)
Common Weakness Enumeration: CWE-807: Reliance on Untrusted Inputs in a Security Decision
This vulnerability is being tracked by BUG 2048764(EOS), BUG 2069205(DMF)

Description

On affected platforms running Arista EOS with 802.1X with Dynamic Host Configuration Protocol (DHCP) device profiling enabled, a network-adjacent attacker can send a crafted DHCP packet to force the device to record a spoofed device profile. This may potentially allow the authenticated supplicant to acquire unauthorized access to a network segment with elevated privileges.

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

- 4.36.2F and earlier release in 4.36.x train
- 4.35.5M and earlier release in 4.35.x train
- 4.34.7M and earlier release in 4.34.x train
- 4.33.9M and earlier release in 4.33.x train
- All releases in the 4.32.x train
- All releases in the End of Support software release train 4.31.x starting from 4.31.2F

Affected Platforms

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 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
  - 7260X/X3 Series
  - 7280R/R2/R3/R4 Series
  - 7050X3/X4 Series
  - 7060X/X2/X4/X5/X6/XE7 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500R/R2/R3 Series
  - 7700R4 Series
  - 7800R3/R4 Series

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

- Arista EOS-based products:
  - 77130 Series running EOS
  - 7170 Series
  - AWE 5000 Series
  - AWE 7200R Series
  - ZTX-7200 Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - CloudVision eXchange, virtual or physical appliance
- Wi-Fi Access Points
- CloudVision CUE cloud service delivery
- CloudVision Portal on-premises, virtual appliance or physical appliance (including the CV-CUE on premises software)
- CloudVision Appliance Software
- CloudVision as-a-Service
- CloudVision AGNI - Cloud service delivery
- CloudVision AGNI - Virtual or physical appliance
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- DANZ Monitoring Fabric (DMF) - Controller Appliance
- DANZ Monitoring Fabric (DMF) - Analytics Node Appliance

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.

- 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-2026-120977, the following condition must be met:

- 802.1X global system authentication control is configured
- **at least one** interface is configured as the 802.1X authenticator
- **at least one** DHCP profiling option is configured
- 802.1X RADIUS accounting is enabled

A supplicant vulnerable to this may be EAPOL or MBA. A sample configuration is given below:

```
switch#show running-config
aaa accounting dot1x default start-stop group radius

dot1x
   ! Any one of the following DHCP profiling options is sufficient;
   ! enabling all three is not required.
   radius av-pair dhcp hostname
   radius av-pair dhcp parameter-request-list
   radius av-pair dhcp vendor-class-id

interface Ethernet5
   switchport mode trunk
   spanning-tree portfast edge
   dot1x pae authenticator
   dot1x port-control auto
dot1x system-auth-control
```

Indicators of Compromise

To determine if this vulnerability has been exploited, inspect RADIUS Accounting messages for

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.

mismatched or unexpected supplicant device profiles, which may lead to incorrect AAA authorization policies or unintended Session Change of Authorization (CoA).

```
switch#show dot1x hosts mac <supplicant_mac> accounting
```

Mitigation

There is no workaround to prevent this behaviour.

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-2026-120977 has been fixed in the following releases:

- 4.37.0F and later release in 4.37.x train
- 4.36.3M and later release in 4.36.x train
- 4.35.6M and later release in 4.35.x train
- 4.34.8M and later release in 4.34.x train
- 4.33.10M and later release in 4.33.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
- By email: support@arista.com
- By telephone: List of regional telephone numbers

Receive notification for new advisories and notices:

Subscribe to the RSS feed and email notifications to receive periodic updates on new software releases, advisories, end of sale and field notices.

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.