Date: September 9, 2026

Revision	Date	Changes
1.0	September 9, 2026	Initial release

Description

All of the CVEs covered in this advisory apply to affected platforms running Arista EOS with 802.1X authentication and authorization enabled and Access Control Lists (ACLs) configured for per-supplicant policy enforcement. An authenticated supplicant on an adjacent network segment may, under specific conditions, send traffic without the intended ACL policy applied, bypassing network segmentation for a brief period. The impact is limited to the integrity of access control enforcement. All issues require 802.1X to be configured in authenticator mode with ACL-based authorization; deployments using 802.1X without per-supplicant ACLs are not affected.

Those issues were discovered internally by Arista, and the company is not aware of any malicious exploitation of these vulnerabilities in customer networks.

CVE-2026-77191

An authenticated supplicant on an adjacent network may bypass intended network authorization policy and send unrestricted traffic during a brief window (milliseconds to seconds) between the completion of the authentication phase and the full enforcement of its assigned ACL.

CVSSv3.1 Base Score: 2.6 (CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N.)
CVSSv4.0 Base Score: 2.1
(CVSS:4.0/AV:A/AC:L/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-862 Missing Authorization
This vulnerability is being tracked by BUG 1108416.

CVE-2026-75943

A brief (milliseconds to seconds) traffic leak may occur when an authenticated supplicant is removed, either via the **clear dot1x host all** CLI command or due to a supplicant timeout. During this window, the supplicant's traffic may pass without ACL enforcement.

CVSSv3.1 Base Score: 2.6 (CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N.)
CVSSv4.0 Base Score: 2.1
(CVSS:4.0/AV:A/AC:L/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-459 Incomplete Cleanup
This vulnerability is being tracked by BUG 1302705.

CVE-2026-75944

A race condition during supplicant re-authentication may leave a stale ACL entry that persists in the system. If the AclAgent subsequently restarts, this stale entry may be applied to new supplicants, resulting in incorrect access control enforcement. User interaction (an AclAgent restart by an administrator) is required for the unintended behavior to take effect.

CVSSv3.1 Base Score: 4.5 (CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H)
CVSSv4.0 Base Score: 5.6
(CVSS:4.0/AV:A/AC:H/AT:P/PR:L/UI:A/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H)
Common Weakness Enumeration: CWE-459 Incomplete Cleanup
This vulnerability is being tracked by BUG 1697612.

CVE-2026-75945

A race condition may cause a supplicant to remain in an authorized state after a clear dot1x host all command is issued.

CVSSv3.1 Base Score: 2.6 (CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N.)
CVSSv4.0 Base Score: 2.1
(CVSS:4.0/AV:A/AC:L/AT:P/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-459 Incomplete Cleanup.
This vulnerability is being tracked by BUG 1857804.

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

CVE-2026-77191

EOS Versions

- 4.35.0.3F and below releases in the 4.35.x train
- 4.34.5M and below releases in the 4.34.x train
- 4.33.7.1M and below releases in the 4.33.x train
- All prior releases

CVE-2026-75943

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

CVE-2026-75944 and CVE-2026-75945

EOS Versions

- 4.36.1F

Affected Platforms

The following products **are** affected by these vulnerabilities:

- 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 these vulnerabilities:

- 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 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 any of the vulnerabilities, the following condition must be met under interface configuration mode:

1. 802.1X (dot1x in the CLI) must be configured with **pae authenticator**
2. port-control must be set to auto mode
3. A static or dynamic ACL must be configured.
4. The RADIUS Access-Accept or Change-of-Authorization (CoA) assigns an ACL to that supplicant using RADIUS AVP (Attribute-Value pair) Filter-Id or NAS-Filter-Rule

Below is an example of one configuration. Note that “mac based authentication always” is optional The supplicant can authenticate with either EAPOL or MBA.

```
switch(config-if-et1)#show active

interface Ethernet5
```

```
   switchport mode trunk
   spanning-tree portfast edge
   dot1x pae authenticator
   dot1x port-control auto

dot1x system-auth-control
```

In this example port control is in “auto” mode, necessary for the condition to occur.

```
config)#show  dot1x  interface  ethernet 5 details
Dot1X Information for Ethernet5
------------------------------------------
Port control: auto
Forced phone authorization: disabled
EAPOL: enabled
Host mode: multi-host
MAC-based authentication: enabled
MAC-based authentication host mode: Unconfigured
MAC-based authentication always: enabled
Quiet period: 60 seconds
TX period: 5 seconds
Maximum reauth requests: 2
Ignore reauth timeout: No
Auth failure VLAN: Unconfigured
Unauthorized access VLAN egress: No
Unauthorized native VLAN egress: No
EAPOL authentication failure fallback: Unconfigured
Port ErrDisabled by CoA: no

Dot1X Authenticator Client
```

Use a preconfigured ACL with which the RADIUS server returns in the **Filter-Id** AVP

```
switch(config)#ip access-list EMPLOYEE-ACL
switch(config-ip-acl-EMPLOYEE-ACL)#10 permit ip 10.0.0.0/8 any
switch(config-ip-acl-EMPLOYEE-ACL)#20 deny ip any any
```

AAA server will return the ACL name through **Filter-Id** AVP through Access-Accept or CoA messages , in the above sample , Filter-Id AVP with EMPLOYEE-ACL will be received from the server.

To verify the configured ACL, execute the following show command to identify the ACL applied to the interface:

```
switch(config)#show ip access-lists interface Ethernet5 summary
IP Access List EMPLOYEE-ACL
   10 permit ip 10.0.0.0/8 any
   20 deny ip any any

   Total rules configured: 2
   Configured on Ingress: Ethernet5
   Active on Ingress: Ethernet5
```

CVE-2026-75945

In addition to the prerequisite above to configure 802.1X in authenticator mode with ACL-based authorization, the supplicant(s) must be removed via the below command:

```
switch(config-dot1x)#clear dot1x host all
```

Indicators of Compromise

CVE-2026-77191

When hardware ACL resources reach capacity during 802.1X bulk authentication and authorization, an authenticated supplicant may temporarily transmit data traffic while authorization is being processed. This condition is signaled by ACL programming failure syslog messages occurring *between* the supplicant's 802.1X authentication and authorization logs, regardless of whether the final authorization succeeds or fails.

```
%DOT1X-6-SUPPLICANT_AUTHENTICATED: Supplicant with identity 001201000002, MAC 0012.01
00.0002 and dynamic VLAN None successfully authenticated on port Ethernet5

Strata: %ACL-3-HW_RESOURCE_FULL: Hardware resources are insufficient to program all A
CLs (Linecard0/0)

SUPPLICANT_FAILED_ACL_AUTHORIZATION: Supplicant with identity 001201000002, MAC 0012.
0100.0002 and dynamic VLAN None successfully authenticated but failed authorization o
n port Ethernet5
```

CVE-2026-75943

No indicators of compromise exist for CVE-2026-75943.

CVE-2026-75944

When hardware ACL resources reach capacity during 802.1X bulk authentication and authorization, attempting to authenticate new supplicants with no ACL or updated ACL configurations may result in stale ACL policies being enforced. This condition is signaled by ACL programming failure syslog messages occurring *between* the supplicant's 802.1X authentication and ACL authorization failure logs.

```
%DOT1X-6-SUPPLICANT_AUTHENTICATED: Supplicant with identity 001201000002, MAC 0012.01
00.0002 and dynamic VLAN None successfully authenticated on port Ethernet5

Strata: %ACL-3-HW_RESOURCE_FULL: Hardware resources are insufficient to program all A
CLs (Linecard0/0)

SUPPLICANT_FAILED_ACL_AUTHORIZATION: Supplicant with identity 001201000002, MAC 0012.
0100.0002 and dynamic VLAN None successfully authenticated but failed authorization o
n port Ethernet5
```

For this issue to occur, Acl Agent restart is required.

```
svd313(config)#  show logging | grep Acl
```

Below are logs we can see after running the show command

```
%PROCMGR-6-PROCESS_TERMINATED: 'Acl'
%PROCMGR-6-PROCESS_STARTED: 'Acl' starting
```

CVE-2026-75945

When a supplicant is removed from 802.1X via the CLI but subsequently continues to display as authenticated, to confirm run ‘show dot1x hosts’ , if the supplicant is not removed then it will still displayed as authenticated only:

```
switch#show dot1x hosts
Port  Supplicant MAC  Username           Auth State    Fallback  VLAN VLAN Name
----- --------------- ------------------ ---- -------  --------- ---- ----------
Et5  0012.0100.0002  arastra  EAPOL  SUCCESS  NONE      30*  VLAN0030
```

Mitigation

CVE-2026-77191, CVE-2026-75943, CVE-2026-75944

There is no workaround available for CVE-2026-77191, CVE-2026-75943, and CVE-2026-75944.

CVE-2026-75945

Re-run the following command to remove all supplicants if the issue persists.

```
switch(config-dot1x)#clear dot1x host all
```

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-2026-77191 has been fixed in the following release:

- 4.35.1F and later releases in the 4.35.x train
- 4.34.6M and later releases in the 4.34.x train
- 4.33.8M and later releases in the 4.33.x train

CVE-2026-75943 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

CVE-2026-75944 and CVE-2026-75945 have been fixed in the following release:

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

Hotfix

No hotfix is available for these issues

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