Date: November 10, 2026

Revision	Date	Changes
1.0	November 10, 2026	Initial release
1.1	November 12, 2026	Clarify details around required configuration and mitigation. Add 720XDM as an impacted platform.

The CVE-ID tracking this issue: CVE-2026-120983
CVSSv3.1 Base Score: 7.6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L)
CVSSv4.0 Base Score: 6.1
(CVSS:4.0/AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N)
Common Weakness Enumeration: CWE-284: Improper Access Control
This vulnerability is being tracked by BUG 903925

Description

On affected EOS platforms where 802.1x is configured in multi-host authenticated mode and the device is configured with Policy Based Routing (PBR), traffic from unauthenticated hosts may not be forwarded as expected. This could potentially allow unauthenticated hosts access to networks. Additionally Layer 2 and Layer 3 control packets from unauthenticated hosts may get copied to the CPU.

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

The following releases of EOS **are** affected:

- 4.36.1F and earlier release in 4.36.x train
- 4.35.5M and earlier release in 4.35.x train

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.

- 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 life software trains

Affected Platforms

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

- 710 Series
- 720D Series
- 720XP/722XPM/720XDM Series
- 7010TX Series
- 7320X Series
- 7060X/X2/X4/X5/X6/XE7 Series
- 7260X/X3 Series
- 7300X/X3 Series
- 7050X3/X4 Series
- 750X Series
- 7250 series
- 7358X4 Series
- 7368X4 Series
- 7388X5 Series

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

- Arista EOS-based products:
  - 7020R/R4 Series
  - 7130 Series running EOS
  - 7170 Series
  - 7280R/R2/R3/R4 Series
  - 7500E/R/R2/R3 Series
  - 7800R3/R4 Series
  - 7700R4 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)

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.

- 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 exploitable, 802.1x has to be configured in multi-host authentication mode along with a PBR policy on the same interface. This also requires at least one host to be authenticated on Dot1x port.

Dot1x Config

Use the show active CLI command in interface config mode, or otherwise view the running configuration, to check if 802.1x is configured in multi-host authenticated mode with the EAPOL authentication method.

For example, the below configuration shows Ethernet21/1 interface with 802.1x configured in multi-host authenticated mode with EAPOL authentication.

```
config#interface Ethernet21/1
config-if-Et21/1#show active
interface Ethernet21/1
   speed forced 100gfull
   switchport access vlan 2
   dot1x pae authenticator
   dot1x port-control auto
   dot1x host-mode multi-host authenticated
```

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.

This issue is present even if MBA is configured, which would appear in the interface mode as dot1x mac based authentication. This is because even with the MBA configured, EAPOL will still be allowed.

Authenticated 802.1X hosts can be listed with:

```
switch#show Dot1x hosts
Port       Supplicant MAC  Username                        Auth   State
     Fallback                VLAN   VLAN Name
---------- --------------- ------------------------------ ------ --------------------
---- ---------------------- ------ ----------
Et21/1     0001.0203.0405  00:01:02:03:04:05              MBA    SUCCESS
     NONE                      2      VLAN0002
Et21/1     a64f.2694.d67d  arastra                        EAPOL  SUCCESS
     NONE                      2      VLAN0002
```

PBR Config:

Use the show policy-map type pbr CLI command to check If PBR config is present. If active routing action is set in the CLI output it means PBR is functioning and will redirect the packet to specified nexthop.

Both Dot1x and PBR must be running on the same VLAN for this issue to occur.

To Check for PBR configuration and identify the active routing action is set and visible:

```
switch# show policy-map type pbr
Service policy PermitAnyPolicy
  Configured on: Vlan2
  Applied on:    Vlan2
  10: Class-map: PermitAnyClass (match-any)
    Match: 10 IP Access List PermitAnyAcl
        counters per-entry
        10 permit ip any any

    Configured actions: set nexthop 30.1.1.2
    Active routing action:
    VRF default
        Route to nexthop 30.1.1.2 default
```

Indicators of Compromise

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.

No indicators of compromise exist.

Mitigation

Configure the PBR policy with specific, trusted address ranges rather than broad match rules. When defining match rules for PBR, only permit IP addresses or ranges that belong to trusted, authenticated hosts. Note: restricting the PBR ACL will affect all traffic matching those rules. Ensure the permitted source ranges include all legitimate authenticated hosts before applying this change.

For example, instead of allowing any source IP address, as described in the requirements for exploitation. The following rule restricts matching strictly to the 20.1.1.0/24 subnet:

```
ip access-list PermitAnyAcl
  counters per-entry
  10 permit ip 20.1.1.0/24 any
```

The issue with control plane packets being forwarded cannot be mitigated. An upgrade to a fixed version of EOS (see “Resolution”) is required in this case.

Resolution

CVE-2026-120983 has been fixed in the following releases:

- 4.37.0F and later release in 4.37.x train
- 4.36.2F 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 vulnerability.

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

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.

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.