Date: May 27, 2025

Revision	Date	Changes
1.0	May 27, 2025	Initial release

The CVE-ID tracking this issue: CVE-2025-2826
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)
Common Weakness Enumeration: CWE-284: Improper Access Control
This vulnerability is being tracked by BUG 795398.

Description

On affected platforms running Arista EOS, ACL policies may not be enforced. IPv4 ingress ACL, MAC ingress ACL, or IPv6 standard ingress ACL enabled on one or more ethernet or LAG interfaces may result in ACL policies not being enforced for ingress packets. This can cause incoming packets to incorrectly be allowed or denied. The two symptoms of this issue on the affected release and platform are:

1. Packets which should be permitted may be dropped and,
2. Packets which should be dropped may be permitted.

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

Vulnerability Assessment

Affected Software

EOS Versions

- 4.33.2F version in the 4.33.x train

Affected Platforms

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

- Arista EOS-based products:
  - 7060X6 Series

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

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.

- 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/X4 Series
    - 7060X/X2/X4/X5 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 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
- Arista Wireless 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
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric (formerly Big Switch BCF)
- Arista DANZ Monitoring Fabric (formerly Big Switch BMF)
- 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)

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.

Required Configuration for Exploitation

In order to be vulnerable to CVE-2025-2826, the following condition must be met: IPv4 ingress ACL, MAC ingress ACL, or IPv6 standard ingress ACL must be configured and active on more than one Ethernet interfaces or one or more LAG interfaces. The output of CLI show commands will look similar to the following:

```
switch> show ip access-lists summary
Phone ACL bypass: disabled
IPV4 ACL default-control-plane-acl [readonly]
        Total rules configured: 27
        Configured on Ingress: control-plane(default VRF)
        Active on     Ingress: control-plane(default VRF)

IPV4 ACL ipv4ACL
        Total rules configured: 2
        Configured on Ingress: Et18/1
        Active on     Ingress: Et18/1
```

or

```
switch>show mac access-lists summary
MAC ACL macAcl
        Total rules configured: 2
        Configured on Ingress: Et18/1
        Active on     Ingress: Et18/1
```

or

```
switch>show ipv6 access-lists summary
Phone ACL bypass: disabled
IPV6 ACL default-control-plane-acl [readonly]
        Total rules configured: 27
        Configured on Ingress: control-plane(default VRF)
        Active on     Ingress: control-plane(default VRF)

Standard IPV6 ACL ipv6StandardACL
        Total rules configured: 2
        Configured on Ingress: Et21/1
        Active on     Ingress: Et21/1
```

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.

If IPv4 Ingress ACL or MAC Ingress ACL or IPv6 standard Ingress ACL are not configured or are not active on any Ethernet interface or LAG interfaces there is no exposure to this issue and the CLI show command output have no active interfaces˜ listed, similar to the following:

```
switch> show ip access-lists summary
Phone ACL bypass: disabled
IPV4 ACL default-control-plane-acl [readonly]
        Total rules configured: 27
        Configured on Ingress: control-plane(default VRF)
        Active on     Ingress: control-plane(default VRF)
```

or

```
switch>show mac access-lists summary
```

or

```
switch>show ipv6 access-lists summary
Phone ACL bypass: disabled
IPV6 ACL default-control-plane-acl [readonly]
        Total rules configured: 27
        Configured on Ingress: control-plane(default VRF)
        Active on     Ingress: control-plane(default VRF)
```

Indicators of Compromise

This vulnerability may lead to unexpected ACL behavior. Examples of misbehaving switches include:

- ACL drops for ingress traffic which should be allowed
- No ACL drops for ingress traffic which should be denied, and traffic reaches devices unexpectedly.

Mitigation

No workaround is available. Ingress ACLs may be applied as egress, if resources permit and the policy is applicable.

Resolution

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 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-2025-2826 has been fixed in the following releases:

- 4.33.2.1F, 4.33.3F and later releases in the 4.33.x train

Hotfix

No hotfix is available. Please upgrade to a release which has the fix for the bug, or downgrade to an earlier supported EOS version.

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

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.