Date: May 20, 2025

Revision	Date	Changes
1.0	May 20, 2025	Initial release

The CVE-ID tracking this issue: CVE-2024-11185
CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Common Weakness Enumeration: CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
This vulnerability is being tracked by BUG1009562

Description

On affected platforms running Arista EOS, ingress traffic on Layer 2 ports may, under certain conditions, be improperly forwarded to ports associated with different VLANs, resulting in a breach of VLAN isolation and segmentation boundaries.

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

- 4.29.10M and below releases in the 4.29.x train
- 4.30.9M and below releases in the 4.30.x train
- 4.31.6M and below releases in the 4.31.x train
- 4.32.3M and below releases in the 4.32.x train
- 4.33.1F and below releases in the 4.33.x train

Affected Platforms

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

- Arista EOS-based products:
  - 7060X5/X6 Series
  - 7388X5 Series

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

- 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 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7500E/R/R2/R3 Series
    - 7800R3/R4 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 and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and 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)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2024-11185, the following condition must be met:

IPV4 or IPV6 routing must be enabled:

```
switch>show vrf
Maximum number of VRFs allowed: 1023
   VRF           Protocols       State         Interfaces
------------- --------------- ---------------- ----------
   default       IPv4            routing    Ma1
   default       IPv6            routing    Ma1
```

Indicators of Compromise

This vulnerability may lead to packets that are expected to be switched in VLAN 1 getting routed to the default VRF instead.

No indicators of compromise exist.

Mitigation

There are no workarounds.

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-2024-11185 has been fixed in the following releases:

- 4.30.10M and later releases in the 4.30.x train
- 4.31.7M and later releases in the 4.31.x train
- 4.32.5M and later releases in the 4.32.x train
- 4.33.2F and later releases in the 4.33.x train

Hotfix

No hotfix exists 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