Date: November 19, 2024

Revision	Date	Changes
1.0	November 19, 2024	Initial release

Description

The CVE-ID tracking this issue: CVE-2024-5872
CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L)
Common Weakness Enumeration: CWE-346: Origin Validation Error
This vulnerability is being tracked by BUG 884202

Description

On affected platforms running Arista EOS, a specially crafted packet with incorrect VLAN tag might be copied to CPU, which may cause incorrect control plane behavior related to the packet, such as route flaps, multicast routes learnt, etc.

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

- 4.32.2F and below releases in the 4.32.x train
- 4.31.4M and below releases in the 4.31.x train
- 4.30.7M and below releases in the 4.30.x train
- 4.29.8M and below releases in the 4.29.x train
- From 4.28.1F through 4.28.11M in the 4.28.x train

Affected Platforms

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

- Arista EOS-based products:
  - 7050X4 Series
  - 7358X4 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 Series
    - 7060X/X2/X4/X5/X6 Series
    - 7250X Series
    - 7260X/X3 Series
    - 7280E/R/R2/R3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7368X4 Series
    - 7388X5 Series
    - 7500E/R/R2/R3 Series
    - 7800R3/R4 Series
    - 7700R4 Series
    - AWE 5000 Series
    - AWE 7200R Series
    - cEOS-lab
    - vEOS-lab
    - CloudEOS
    - CloudVision eXchange, virtual or physical appliance
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi 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)

Required Configuration for Exploitation

There are multiple conditions which must be met. An L3 interface must be configured on the device and at least one of four additional conditions, detailed below and labeled 1 through 4, must be met. In addition to the configuration the packet being sent must have an incorrect VLAN tag.

In order to be vulnerable to CVE-2024-5872, an L3 interface MUST be configured on the device.

To check IPv4 L3 interface configuration:

```
Switch>show ip interface brief
                                                                  Address
Interface      IP Address          Status     Protocol      MTU   Owner
-------------- ------------------- ---------- ---------- ------ -------
Ethernet5/1    5.1.1.1/24          up         up           1500
Management1    10.240.112.30/25    up         up           1500
Vlan4          4.1.1.1/24          up         up           1500
```

To check IPv6 L3 interface configuration:

```
Switch>show ipv6 interface brief
Interface  Status  MTU IPv6 Address             Addr State Addr Source
---------- ------- ---- ------------------------ ---------- -----------
Ma1        up     1500 fe80::d3ff:fe5f:73e9/64 up         link local
                       fdfd:5c41:712d::701e/64 up         config
Vl4        up     1500 fe80::d3ff:fe5f:73ea/64 up         link local
                       120::1/120               up         config
```

AND

At least one of the following conditions (#’s 1-4 below) must be met:

1. Either IPv4 routing or IPv6 routing is not configured, which will cause the vulnerability to impact IPv4 unicast packets or IPv6 unicast packets, respectively:

```
Switch>show ip

IP Routing : Disabled
IP Multicast Routing : Disabled
IPv6 Multicast Routing : Disabled
IPv6 Interfaces Forwarding : None
```

```
IPv6 Unicast Routing : Disabled
```

OR

2. For packets with TTL of 0 or 1, all IP configurations are vulnerable.

OR

3. Unicast and multicast routing must be configured for IPv4 to be vulnerable for IPv4 multicast packets, and IPv4 multicast must be enabled on an L3 interface:

```
Switch>show ip

IP Routing : Enabled
IP Multicast Routing : Enabled
IPv6 Multicast Routing : Disabled
IPv6 Interfaces Forwarding : None

IPv6 Unicast Routing : Disabled
Switch(config-if-Vl4)#show active
interface Vlan4
   ip address 4.1.1.1/24
   pim ipv4 sparse-mode
```

OR

4. Unicast and multicast routing must be configured for IPv6 to be vulnerable to IPv6 multicast packets, and IPv6 multicast must be enabled on an L3 interface:

```
Switch>show ip

IP Routing : Disabled
IP Multicast Routing : Disabled
IPv6 Multicast Routing : Enabled
IPv6 Interfaces Forwarding : None
```

```
IPv6 Unicast Routing : Enabled
Switch(config-if-Vl4)#show active
interface Vlan4
   ipv6 address 120::1/120
   pim ipv6 sparse-mode
```

Indicators of Compromise

This vulnerability can cause CPU counters to increment unexpectedly. An indication of this issue is the TTL1 or Multicast Miss queues show an unexpected increase in the rate of packets forwarded by the CPU.

```
Switch>show cpu counters queue | nz
------------------------------------------------------------------------
                     Linecard0/0
------------------------------------------------------------------------
Queue                              Counters/pkts          Drops/pkts
------------------------------------------------------------------------
TTL1                                        2                 0
Multicast Miss                              8                 0
```

This vulnerability can cause packet traces to increment unexpectedly. A packet that unexpectedly increments the following drop counter and one of the two trace counters may indicate the issue (privileged mode required):

```
Switch#platform trident diag estat show trace
RX Trace Event Counters :
    L3_TTL_ERROR                                :               10
    L3_DST_LOOKUP_MISS                          :               10

Switch#platform trident diag estat show drop
RX Drop Event Counters :
    MEMBERSHIP_CHECK_FAILED                     :               18
```

There is no direct indicator of compromise. It is possible for the above indicators to occur as part of a false positive.

Control plane policies can be used to protect the CPU from potential Denial of Service attacks caused by processing too many packets.

Mitigation

There is no workaround.

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-2024-5872 has been fixed in the following releases:

- 4.33.0F and later releases in the 4.33.x train
- 4.32.3M and later releases in the 4.32.x train
- 4.31.5M and later releases in the 4.31.x train
- 4.30.8M and later releases in the 4.30.x train
- 4.29.9M and later releases in the 4.29.x train
- 4.28.12M and later releases in the 4.28.x train

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