Date:December 16th, 2020

Version: 1.0

Revision	Date	Changes
1.0	December 16th, 2020	Initial Release

The CVE-ID tracking this issue: CVE-2020-26569
CVSSv3.1 Base Score: 5.9/10 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

Description

This advisory documents the impact of a vulnerability in Arista's EOS involving crossing VLAN boundaries in X-series platforms identified under "Symptoms", and "Affected Platforms" below.

In EVPN VxLAN setups, the effect of this vulnerability is that specific malformed packets can lead to incorrect MAC to IP bindings and as a result packets can be incorrectly forwarded across VLAN boundaries. This can result in traffic being discarded on the receiving VLAN.

Please note that this advisory does not refer to the crossing of VLAN boundaries as a result of the explicit configuration of inter-VLAN routing, which would be expected behavior.

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

- 4.21.12M and below releases in the 4.21.x train.
- 4.22.7M and below releases in the 4.22.x train.
- 4.23.5M and below releases in the 4.23.x train.
- 4.24.2F and below releases in the 4.24.x train.

Affected Platforms

- The following products are affected by this vulnerability:
    - 7010 series
    - 7050X/X2/X3 series
    - 7060X/X2/X4 series

    - 720X series
    - 7250X series
    - 7260X/X3 series
    - 7300X/7320X/7300X3 series
    - 7368X4 series

- The following products are not affected:
    - Arista Wireless Access Points
    - CloudVision Wi-Fi (on-premise and cloud service delivery)
    - CloudVision Portal, virtual appliance or physical appliance
    - CloudVision and the CV Servers
    - CloudVision as-a-Service
    - CloudEOS Virtual Router, as a VM on-premises or in the public cloud marketplaces
    - CloudEOS Container, that runs in Kubernetes on-premises clusters
    - Arista 7130 Systems running MOS
    - Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
    - Arista EOS-based products:
        - 750 series
        - 7150 series
        - 7160 series
        - 7170 series
        - 7020R Series
        - 7280E/R/R2/R3 series
        - 7500E/R/R2/R3 series
        - 7800R3 series

Symptoms

Affected platforms are vulnerable when deployed in an EVPN VxLAN design with SVIs (Switched VLAN Interfaces) configured. If unexpected traffic loss is noticed, this vulnerability can be verified by checking for invalid bindings between the IP and MAC address for each VLAN.

To verify if a device is vulnerable, use the commands in the following example to identify the presence of EVPN VxLAN configuration with SVIs.

- Check for EVPN and VxLAN configuration

```
router bgp 65006

   !
   vlan 8
      rd 65006:500150
      route-target both 65006:500150
```

```
      redistribute learned
   !
   address-family evpn
      neighbor 1.1.1.1 activate
```

Figure-1: EVPN configuration snippet

In the configuration snippet present in Figure-1, address-family evpn has been configured under the "router bgp" configuration context. Additionally, the EVPN address-family has been activated for a peer as indicated by the "neighbor 1.1.1.1 activate " piece of configuration . This indicates that EVPN has been configured on the Switch in question. Please note that the EVPN address-family can be activated for multiple peers as well.

```
Switch#show running-config section vxlan

interface Vxlan1
   vxlan source-interface Loopback0
   vxlan udp-port 4789
   vxlan vlan 8 vni 800
```

Figure-2: VxLAN configuration

The presence of a VxLAN interface configuration as shown in Figure-2 confirms that VxLAN is enabled.

- Check for configured SVIs

```
Switch#show vlan
VLAN  Name                              Status    Ports
----- --------------------------------- --------- -------------------------
----------
8
                    active    Cpu, Et1, Et2, Vx1
```

Figure-3: show vlan output

In the output of "show vlan" as shown in Figure-3, if "Cpu" is listed under "Ports" for any VLAN, it means that a SVI has been configured for the VLAN in question. In the above example, there

is an SVI configured in VLAN8 which makes VLAN 8 vulnerable even if it does not map to any VNIs.

In the scenario of unexpected traffic loss, the ARP/ND tables can be further reviewed to identify any invalid IP to MAC bindings.The following commands and output example (Figure-4) can be used to confirm if there are any invalid or unexpected IP-MAC bindings.

```
Switch#show arp
Address         Age (min)  Hardware Addr   Interface
10.64.139.65          N/A  aaaa.aaaa.aaa  Vlan8, Not learned

Switch#show ipv6 neighbors
IPv6 Address                              Age Hardware Addr    State I
nterface
2001::2                                   N/A aaa1.aaa1.aaa1   REACH V
l8, not learned
```

Figure-4: show arp/show ipv6 neighbors output

If the host with the IP address in the ARP entry is actively sending traffic and the output of the ARP/Neighbor discovery table shows the entry as 'not learned', this is a possible indication that the entry was incorrectly updated as a result of this vulnerability.

Mitigation

A mitigation for this is to first identify the malicious sending IP and then clear the corresponding entry from the ARP/IPv6 neighbor table.

For the final resolution, please refer to the next section which lists the details of the remediated software versions.

Resolution

This vulnerability is being tracked by BUG 407644. The recommended resolution is to upgrade to a remediated EOS version, listed below.

- 4.21.13M
- 4.22.8M
- 4.23.6M
- 4.24.3M
- 4.25.0F

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: 408-547-5502
866-476-0000