Date:December 16th, 2020

Version: 1.0

Revision	Date	Changes
1.0	December 16th, 2020	Initial Release

The CVE-ID tracking this issue: CVE-2020-15898
CVSSv3 Base Score: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)

Description

This advisory documents the impact of a vulnerability in Arista's EOS involving crossing VLAN boundaries in X-Series and 7170 Series platforms identified below. To evaluate if a system is vulnerable please see the "Symptoms" section below for specific required configuration.

The effect of this vulnerability is that malformed packets can be incorrectly forwarded across VLAN boundaries in one direction. This vulnerability is only susceptible to exploitation by unidirectional traffic (ex. UDP) and not bidirectional traffic (ex. TCP).

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

- 7170 platforms:
  - 4.21.4.1F and below releases in the 4.21.x train.
- For all X-Series:
  - 4.21.11M and below releases in the 4.21.x train.
  - 4.22.6M and below releases in the 4.22.x train.
  - 4.23.4M and below releases in the 4.23.x train.
  - 4.24.2.1F 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
  - 7170 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
    - 7020R Series
    - 7280E/R/R2/R3 series
    - 7500E/R/R2/R3 series
    - 7800R3 series

Symptoms

Evaluation for the X-Series

For the **X-Series**, this vulnerability is applicable to systems configured with VLAN interfaces (SVIs) where the SVI is assigned to a VRF with ip routing disabled. The following command can be used to confirm the VLAN(s) exposed to this vulnerability for all X-Series platforms.

Using the output of **show vrf** (Figure 1, below), confirm if IPv4 or IPv6 routing has been disabled for the VRF and if the VRF has SVIs assigned. Please note that the text highlighted in red refers to vulnerable configuration and the text highlight in blue refers to configuration that is NOT vulnerable.

In the following example,

- Vlan 1 is vulnerable in the 'default' VRF as IPv4 routing is disabled (even if IPv6 routing is enabled) and the L3 interface list includes the SVI for VLAN 1
- Vlan 10 is vulnerable in the 'test1' VRF as IPv6 routing is disabled (even if IPv4 routing is enabled) and the L3 interface list includes the SVI for VLAN 10
- Vlan 20 is not vulnerable in the 'test2' VRF even with a VLAN interface as IPv4 **and** IPv6 routing are enabled in this VRF

```
Switch#show vrf
Maximum number of vrfs allowed: 1023
   VRF           RD              Protocols       State          Interf
aces
------------ -------------- -------------- ----------------- ------
--------------------
   default
                        ipv4,ipv6
  v4:no routing,    Vlan1, Ethernet8/1,
                                              v6:routing        Ethern
et9/1, Loopback0,


   test1
         100:1
          ipv4,ipv6    v4:routing,      Vlan10, Ethernet3/1,

                       v6:no routing    Ethernet7/1, Loopback1

   test2
         200:1           ipv4,ip
v6    v4:routing,      Vlan20, Ethernet4/1,

                       v6:routing       Ethernet8/1, Loopback2
```

Figure-1: show vrf output

In EOS releases prior to 4.23.x, the VRF default interfaces are not listed in the output of the **show vrf** command. If the X-Series device in question is running a release prior to 4.23.x, please use the following commands to identify VLANs in the **default VRF** that are vulnerable. For non-default VRFs, continue to use the output of 'show vrf' as described using Figure-1 above.

- To check the status of IPv4 routing in the 'default' VRF, use the command 'show running-configuration section ip routing'

```
Switch#show running-configuration section ip routing

no ip routing
no ip routing vrf test1
ip routing vrf test2
```

Figure-2: Check for IPv4 routing in default VRF

In the example above (Figure-2), the highlighted configuration indicates that IPv4 routing is disabled in the 'default' VRF.

- To check the status of IPv6 routing in the 'default' VRF, use the command 'show running-configuration all section ipv6 unicast-routing':

```
Switch#show running-config all section ipv6 unicast-routing
no ipv6 unicast-routing
no ipv6 unicast-routing vrf test1
no ipv6 unicast-routing vrf test2
```

Figure-3: Check for IPv6 routing in default VRF

In the example above (Figure-3), the highlighted configuration indicates that IPv6 routing is disabled in the 'default' VRF.

To check if the 'default' VRF has configured SVIs, use the command 'show ip interface vrf default'

```
Switch#show ip interface vrf default

Vlan1 is up, line protocol is up (connected)
### Output omitted for brevity ###
```

Figure-4: Check for SVIs configured in default VRF

In the above example (Figure-4), VLAN1 has an SVI configured.

Evaluation for 7170 Platforms

On the 7170 series, systems running the affected software version are vulnerable if SVIs are configured for VLANs. The check for IP routing is not required for this platform.

To confirm if an SVI has been configured for any VLAN use the command 'show vlan'

```
Switch#show vlan
VLAN  Name                              Status    Ports
----- --------------------------------- --------- -------------------
----------
1     default                           active    Cpu, Et2/1, Et4/1


```

Figure-5: SVI check for 7170

In the above example (Figure-5), "Cpu" is listed under "Ports" for VLAN 1 indicating that an SVI is configured in VLAN 1. 7170 systems are vulnerable if an SVI is configured in **any** VLAN.

Mitigation

For the X-series platforms, the mitigation step is to enable IP routing for the VRFs in question.

- To enable IP routing in the default VRF, use the command 'ip routing' from the configuration mode
- To enable IP routing in non-default VRFs, use the command 'ip routing vrf ' from the configuration mode

There is no mitigation available for the 7170 platforms.

Resolution

This vulnerability is being tracked by Bugs 359990 and 360186. The recommended resolution is to upgrade to a remediated EOS version.

- For X-Series platforms, the vulnerability has been fixed in the following EOS versions:
    - 4.21.6.4F
    - 4.21.12M
    - 4.22.7M
    - 4.23.5M
    - 4.24.3M
    - 4.25.0F
    - Special releases
        - 4.21.2.7F
        - 4.24.2.2F
- For 7170 platforms, the vulnerability has been fixed in 4.21.5F and above releases in the

4.21.x train. Note that the 7170 platforms running versions in EOS release trains 4.22.x, 4.23.x and 4.24.x are not affected.

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