Date:December 16th, 2020

Version: 1.0

Revision	Date	Changes
1.0	December 16th, 2020	Initial Release

The CVE-ID tracking this issue: CVE-2020-26568
CVSSv3.1 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 for device configurations leveraging VxLAN Routing and VRFs. To evaluate if a VxLAN enabled device is vulnerable, please see the "Symptoms" section below for details.

On impacted devices, malformed packets could be incorrectly forwarded across VRF boundaries when non-default VRFs are configured. This issue affects UDP traffic, and will fail to complete the three-way handshake for TCP traffic.

Please note that this advisory does not refer to the crossing of VRF boundaries as a result of the configuration of inter-VRF 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
  - 4.21.12M and below releases in the 4.21.x train.
  - 4.22.7M and below releases in the 4.22.x train.
  - 4.23.4M 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:
  - 7280E/R/R2 series
  - 7020R Series
  - 7500E/R/R2 series

    - 7050X/X2/X3 series
    - 7060X/X2 series
    - 7160 series
    - 7170 series
    - 720X series
    - 750x series
    - 7250X/7250X2 series
    - 7260X/X3 series
    - 7300X/X3 series
    - 7320X series
    - CloudEOS Virtual Router, as a VM on-premises or in the public cloud marketplaces
    - CloudEOS Container, that runs in Kubernetes on-premises clusters

- The following products are not affected:
    - Arista 7130 Systems running MOS
    - Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
    - 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
    - Arista EOS-based products:
    - 7010 series
    - 7150 series
    - 7280R3/ 7500R3 / 7800R3 series
    - 7060X4 Series
    - 7368X4 series

Symptoms

This vulnerability is applicable to systems with both non-default VRFs and VxLAN configured. The exploitation of this vulnerability would result in packets crossing VRF boundaries in one direction.:

To confirm if the vulnerability is applicable, the following checks can be performed by logging into the device in question. :

1) Confirm if non-default VRF(s) has been configured via the command **show vrf:**

Example:

```
Switch#show vrf
Maximum number of vrfs allowed: 1023
   VRF           RD              Protocols       State          Interf
```

```
aces
------------- --------------- --------------- ----------------- ------
--------------------
   default                         ipv4,ipv6       v4:routing,    Vlan1,
 Ethernet8/1,
                                                   v6:routing     Ethern
et9/1, Loopback0,


   test1
         100:1           ipv4,ipv6       v4:routing,    Vlan10, Ethern
et3/1,
                                                   v6:routing     Ethern
et7/1, Loopback1

   test2
         200:1           ipv4,ipv6       v4:routing,    Vlan20, Ethern
et4/1,
                                                   v6:routing     Ethern
et8/1, Loopback2
```

2) Confirm if VXLAN has been configured:

Example:

```
Switch#show running-config section vxlan

interface Vxlan1
   vxlan source-interface Loopback0
   vxlan udp-port 4789
   vxlan vlan 10 vni 100
   vxlan vrf test1 vni 1001
```

Mitigation

There is no mitigation available to address this vulnerability. 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 485689. The recommended resolution is to upgrade

to a remediated EOS version during a maintenance window.

The vulnerability is fixed in the following EOS versions:

- 4.21.13M
- 4.22.7.1M
- 4.23.5M
- 4.24.3M
- 4.25.0F
- Special releases:
    - 4.24.2.2F

Post upgrade impact on select platforms:

This section of the advisory applies to the following list of platforms:

- 7050X/X2/X3 series
- 7060X/X2 series
- 7160 series
- 7170 series
- 720x series
- 750x series
- 7250X/7250X2 series
- 7260X/X3 series
- 7300X/X3 series
- 7320X series

For customers whose network design leverages VxLAN decapsulation on an interface that carries traffic for multiple VRFs, the following additional steps may be required post EOS upgrade.

Once an upgrade to a release with the fix has been completed, the following warnings may be logged under "show logging all":

```
%VXLAN-4-DECAPSULATION_DISABLED:
 VXLAN decapsulation has been disabled on
Ethernet48 because it carries both default VRF and non-
default VRF traffic
```

```
%VXLAN-4-DECAPSULATION_DISABLED:
 VXLAN decapsulation has been disabled on Ethernet48 because it carrie
s non-default VRF traffic
To allow VXLAN decapsulation on interfaces that carry both default VRF
 and non-default VRF traffic issue the command: 'vxlan decapsulation f
```

```
ilter interface multiple-vrf disabled'.
To entirely disable VRF-based VXLAN decapsulation filtering on this sw
itch/router, configure 'vxlan decapsulation filter disabled'.
```

If the above warnings have been observed, it indicates that VxLAN decapsulation has been disabled on the listed interfaces (for example, in the above case VxLAN decapsulation has been disabled on ethernet48).

These warnings and the associated action of disabling VxLAN decapsulation can be expected post an upgrade. The next step would be to confirm if one of interfaces included in these warnings is a "core-facing interface". A core-facing interface is the physical port on which the switch receives VxLAN encapsulated traffic from remote VTEPs. Please note that the core-facing interface is not determined on the basis of any configuration, rather it is the result of the network design.

A core-facing interface is typically the uplink to a Spine in a Leaf-Spine topology. In order to enable VxLAN decapsulation on a core-facing interface, the following configuration can be applied under the "interface vxlan 1" configuration context.

Please note that the application of the configuration below will revert the default behavior for the interfaces specified in the "interface list". This configuration only needs to be applied if VxLAN decapsulation has been disabled on the core-facing interfaces (or any physical interface on which it is expected to receive and decapsulate VxLAN traffic). **This configuration can be disregarded if it is not expected to receive and decapsulate VxLAN traffic on a physical interface that carries traffic for multiple VRFs.**

vxlan decapsulation filter interface multiple-vrf disabled []

Example:

```
(config-if-Vx1)# vxlan decapsulation filter interface multiple-
vrf disabled Ethernet48
```

If there are multiple core-facing interfaces (i.e. multiple uplinks to the spine), all relevant interfaces will need to be specified.

Example:

```
(config-if-Vx1)# vxlan decapsulation filter interface multiple-
vrf disabled Ethernet48 Ethernet49
```

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