Date: August 23, 2023

Revision	Date	Changes
1.0	August 23, 2023	Initial release

The CVE-ID tracking this issue: CVE-2023-24548
CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
Common Weakness Enumeration: CWE-120 Buffer Copy without Checking Size of Input
This vulnerability is being tracked by BUG 828687

Description

On affected platforms running Arista EOS with VXLAN configured, malformed or truncated packets received over a VXLAN tunnel and forwarded in hardware can cause egress ports to be unable to forward packets. The device will continue to be susceptible to the issue until remediation is in place.

The issue was discovered in an Arista customer environment but Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.25.0F in the 4.25.x train
- 4.24.11M and below releases in the 4.24.x train
- 4.23.14M and below releases in the 4.23.x train
- 4.22.13M and below releases till 4.22.1F in the 4.22.x train

Affected Platforms

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

- Arista EOS-based products:
    - 7280R3 Series
    - 7500R3 Series
    - 7800R3 Series

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

- Arista EOS-based products:
  - 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/X5 Series
  - 7250X Series
  - 7260X/X3 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - AWE 5000 Series
- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- 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

In order to be vulnerable to CVE-2023-24548, the following three conditions must be met:

IP routing should be enabled:

```
Switch> show running-config section ip routing
ip routing
```

AND

VXLAN should be configured - a sample configuration is found below:

```
# Loopback interface configuration
switch> show running-config section loopback
interface Loopback0
   ip address 10.0.0.1/32

# VXLAN VTEP configuration
switch> show running-config section vxlan
interface Vxlan1
   vxlan source-interface Loopback0
   vxlan udp-port 4789
   vxlan flood vtep 10.0.0.2
```

AND

VXLAN extended VLAN or VNI must be routable - two examples are shown below:

```
# Overlay interface
switch> show running-config section vlan
vlan 100
interface Ethernet1/1
   switchport access vlan 100
interface Vlan100
   ip address 1.0.0.1/24

Interface Vxlan1
  vxlan vlan 100 vni 100000
```

```
switch> show running-config section red
vrf instance red
ip routing vrf red

interface Vxlan1
   vxlan vrf red vni 200000
```

Whether such a configuration exists can be checked as follows:

```
switch> show vxlan vni
VNI to VLAN Mapping for Vxlan1
VNI          VLAN       Source       Interface         802.1Q Tag
------------ ---------- ------------ ----------------- ----------
100000       100        static       Ethernet1/1       untagged
                                     Vxlan1            100

VNI to dynamic VLAN Mapping for Vxlan1
VNI          VLAN       VRF       Source
------------ ---------- --------- ------------
200000       1006       red       evpn

switch> show vlan
VLAN  Name                             Status    Ports
----- -------------------------------- --------- ---------------------
----------
100   VLAN0100                         active    Cpu, Vx1
1006* VLAN1006                         active    Cpu, Vx1

switch> show ip interface brief

         Address
Interface         IP Address            Status       Protocol
   MTU    Owner
----------------- --------------------- ------------ -------------- --
--------- -------
Vlan100
           1.0.0.1/24           up           up                  1500
Vlan1006
```

```
          unassigned            up           up                10168
```

From the above outputs, it can be seen that IP routing is enabled, VXLAN is configured, and VNIs 100000 (mapped to VLAN 100) and 200000 (mapped to VRF red) are routable.

Indicators of Compromise

This vulnerability causes egress ports to stop passing traffic. An indication of this issue is that the interface counters for the impacted egress interfaces would no longer increment even if packets are forwarded to those ports.

```
switch > show interfaces counters | nz
Port                          OutOctets    OutUcastPkts    OutMcastPkt
s    OutBcastPkts
Et8/1                            139851
               0            1137               0
```

We will also see the DeqDeletePktCnt go up in show hardware counter drop.

```
switch > show hardware counter drop | nz
Summary:
Total Adverse (A) Drops: 2033
Total Packet Processor (P) Drops: 0
Type  Chip         CounterName                    :           Count :
First Occurrence    : Last Occurrence
----------------------------------------------------------------------
----------------------------------------
A     Fap0         DeqDeletePktCnt
                :          2033
 : 2023-04-05 10:09:17 : 2023-04-05 10:10:51
```

In addition, protocols that establish neighbor relationships over the affecting port are likely to be affected.

Mitigation

There is no known mitigation for the issue. The recommended resolution is to upgrade to a remediated software version at your earliest convenience.

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-2023-24548 has been fixed in the following releases:

- 4.30.0F and later releases in the 4.30.x train
- 4.29.0F and later releases in the 4.29.x train
- 4.28.0F and later releases in the 4.28.x train
- 4.27.0F and later releases in the 4.27.x train
- 4.26.0F and later releases in the 4.26.x train
- 4.25.1F and later releases in the 4.25.x train

No remediation is planned for EOS software versions that are beyond their standard EOS support lifecycle (i.e. 4.22, 4.23).

Hotfix

No hotfix is available for this vulnerability.

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
Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support