Date: April 1st, 2022

Revision	Date	Changes
1.0	April 1st, 2022	Initial Release

The CVE-ID tracking this issue: CVE-2021-28504
CVSSv3.1 Base Score: 7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
Common Weakness Enumeration: CWE-284 Improper Access Control
This vulnerability is being tracked by BUG 614735

Description

On affected platforms running Arista EOS, deny rules fail to get applied for packets of size higher than the configured maximum transmission unit (MTU), which results in packets of large size getting routed by the switch.

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

- 4.27.1F and below releases in the 4.27.x train
- 4.26.3M and below releases in the 4.26.x train
- 4.25.6M and below releases in the 4.25.x train

Affected Platforms

The following products are affected by this vulnerability:

- CCS-750 series
- CCS-722XPM-48Y4-F
- CCS-722XPM-48ZY8-F
- DCS-7010TX-48 series

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

- Arista EOS-based products:
    - 7010T series
    - 7020R series
    - 7050X/X2/X3/X4 series
    - 7060X/X2/X3/X4/X5 series

    - 7130 series
    - 7150 series
    - 7160 series
    - 7170 series
    - 720XP series
    - 7250X series
    - 7260X/X3 series
    - 7280E/R/R2/R3 series
    - 7300X/X3 series
    - 7320X series
    - 7358X4 series
    - 7368X4 series
    - 7388X5 series
    - 7500E/R/R2/R3 series
    - 7800R3 series
- 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
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Awake Security Platform

Required Configuration for Exploitation

In order to be vulnerable to CVE-2021-28504 the following conditions must be all be met:

Routing should be enabled on the switch. To determine if routing is enabled on the switch,

```
switch# show running-config  | include ip routing
ip routing
```

Layer3 interfaces must be active. To determine if L3 interfaces exist on the switch,

```
switch# show ip interface brief | exclude  Management

   Address
Interface           IP Address             Status       Protocol                MTU
   Owner
------------------- ---------------------- ------------ -------------------- --------
-- -------
Vlan1000            unassigned             up           up                     1500
```

Ingress data plane ACL should be applied to routed port / SVI. Run the following command to determine if “active on ingress” line has one or more L3 interfaces

```
switch# show ip access-lists deny summary

IPV4 ACL deny
        Total rules configured: 1
        Configured on Ingress: Et1/1,Vl1000
        Active on     Ingress: Et1/1,Vl1000

switch #show ip access-lists deny
IP Access List deny
        1 permit tcp any eq bgp any
        2 permit tcp any any eq bgp
        3 permit udp any any eq 179
        4 permit udp any eq 179 any
        10 deny ip any any
```

Indicators of Compromise

There are no indicators in logs and syslogs.

If configurations above are all met then, there is a potential for packets with length greater than configured / default MTU to be fragmented and routed via control-plane.

To check CPU forwarding run `*show cpu counters queue | nz*`. If `*L3 Slow Path*` queue shows an unexpected increase in the rate of packets forwarded by the CPU then this may be an indication of the issue.

```
switch# show cpu counters queue | nz
------------------------------------------------------------------------------------------
----------
                                    SwitchcardCes1/0
------------------------------------------------------------------------------------------
----------
Queue                                          Counters/pkts          Drops/pkts
------------------------------------------------------------------------------------------
----------


------------------------------------------------------------------------------------------
----------
                                    SwitchcardCes2/0
```

```
-------------------------------------------------------------------------------
----------
Queue                                       Counters/pkts          Drops/pkts
-------------------------------------------------------------------------------
----------
L3 Slow Path                                      100                    0
```

Mitigation

There is no mitigation / workaround for this issue.

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.

CVE-2021-28504 has been fixed in the following releases:

- 4.27.2F and later releases in the 4.27.x train
- 4.26.4M and later releases in the 4.26.x train
- 4.25.7M and later releases in the 4.25.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:

By email: support@arista.com

By telephone: 408-547-5502 ; 866-476-0000