Date: March 29th, 2022

Version: 1.0

Revision	Date	Changes
1.0	March 29th, 2022	Initial Release

The CVE-ID tracking this issue: CVE-2021-28505
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 609752

Description

On affected Arista EOS platforms, if a VXLAN match rule exists in an IPv4 access-list that is applied to the ingress of an L2 or an L3 port/SVI, the VXLAN rule and subsequent ACL rules in that access list will ignore the specified IP protocol.

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:

- 4.26.3M and below releases in the 4.26.x train
- 4.27.0F in the 4.27.x train

Affected Platforms

The following products are affected by this vulnerability:

- CCS-710P-12
- CCS-710P-16P
- CCS-720XP-24Y6
- CCS-720XP-24ZY4
- CCS-720XP-48Y6
- CCS-720XP-48ZC2
- CCS-720XP-96ZC2
- CCS-722XPM-48Y4
- CCS-722XPM-48ZY8
- DCS-7010TX-48

- DCS-7050CX3-32S
- DCS-7050CX3M-32S
- DCS-7050SX3-48C8
- DCS-7050SX3-48YC8
- DCS-7050SX3-48YC12
- DCS-7050SX3-96YC8
- DCS-7050TX3-48C8

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

- Arista EOS-based products:
    - 7010T series
    - 7020R series
    - 7050X/X2/X4 series
    - 7060X/X2/X3/X4/X5 series
    - 7130 series
    - 7150 series
    - 7160 series
    - 7170 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

On impacted products listed in the “Impacted Products” section above, if a TCAM profile is enabled - including the default profile - the device is impacted by CVE-2021-28505. Also a log message created when configuration is created.

The steps below can be used to confirm a vulnerable configuration is present.

To confirm that the default TCAM profile is enabled and has the potential to cause this issue, run the following commands;

1. The following indicates that TCAM profile is enabled and profile “foo” is active.

```
switch# show hardware tcam profile
                     Configuration           Status
FixedSystem          foo                     foo
```

2. The command below captures a snip of TCAM profile “foo” configuration. If the output of the command is either,

a. empty as shown below, or

```
switch# show hardware tcam profile foo detail | grep -A4 "acl port ip
ingress"
switch#
```

b. has the key-field “ip-protocol” then please proceed with further verification steps to confirm if issue is present. If the key-field “ip-protocol” does not exist, then this issue does not impact you.

```
switch# show hardware tcam profile foo detail | grep -A4 "acl port ip
ingress"
 Feature:               acl port ip ingress
 Key size:              320
 Key Fields:
 dscp, dst-ip, ip-frag, ip-protocol, l4-dst-port,
                        l4-ops, l4-src-port, src-ip, tcp-control, ttl
```

To check if any of the configured access-lists can potentially run into this issue run the following command,

```
switch# show ip access-
lists | grep -E "IP Access List | permit vxlan | deny vxlan"

switch(config)#show ip access-
lists | grep -E "IP Access List | permit vxlan | deny vxlan"
```

```
IP Access List default-control-plane-acl [readonly]
IP Access List test
    20 permit vxlan any any
```

if any lines have "permit / deny vxlan" then check the "IP Access List" line to figure out the access-list names.

From the access-list names check output of following command,

```
switch# show ip access-lists summary

switch(config)#sh ip access-lists summary
IPV4 ACL test
    Total rules configured: 4
    Configured on Ingress: Et1/1
    Active on     Ingress: Et1/1
```

if the potential access-lists have "Active on Ingress:" in output then the issue is confirmed.

Resultant Impact

On affected products listed above which have the “TCAM profile” feature enabled, any IPv4 access-list that has a rule which matches on “vxlan” as protocol then that rule and subsequent rules (rules declared after it in ACL) do not match on IP protocol field as expected.

Indicators of Compromise

On affected products, the vulnerability ignores the IP protocol specified in the VXLAN rule and subsequent rules of the IPv4 access list. This can result in unexpected traffic flows that were otherwise expected to be filtered by the access list. In the following example, rule 20 matches VXLAN traffic. An affected device would ignore the IP protocol field in rules 20 and 30 resulting in allowing any IP traffic.

```
switch# ip access-list test
   10 permit tcp any any
   20 permit vxlan any any
   30 permit udp any any
   40 deny icmp any any
```

Mitigation

Replace "vxlan" IP protocol match with match on IP protocol "udp" and Layer 4 destination port for VxLAN encapsulated packets i.e 4789. < br/> If VXLAN L4 destination port number is not the default 4789 then use the configured L4 destination port number.

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-2021-28505 has been fixed in the following releases:

- 4.26.4M and later releases in the 4.26.x train
- 4.27.1F and later releases in the 4.27.x train

Hotfix

No hotfix is available for this issue.

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