Date: July 19th, 2022

Revision	Date	Changes
1.0	July 19th 2022	Initial release

The CVE-ID tracking this issue: CVE-2021-28511
CVSSv3.1 Base Score: 5.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N)
Common Weakness Enumeration (CWE): CWE-284 Improper Access Control
The internal bug tracking this issue: BUG 641088

Description

This advisory documents the impact of an internally found vulnerability in Arista EOS for security ACL bypass.

The impact of this vulnerability is that the security ACL drop rule might be bypassed if a NAT ACL rule filter with permit action matches the packet flow.

This could allow a host with an IP address in a range that matches the range allowed by a NAT ACL and a range denied by a Security ACL to be forwarded incorrectly as it should have been denied by the Security ACL. This can enable an ACL bypass.

This issue was discovered internally and Arista is not aware of any malicious use of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS:

- 4.24.9 and below releases in the 4.24.x release train
- 4.25.8 and below releases in the 4.25.x release train
- 4.26.5 and below releases in the 4.26.x release train
- 4.27.3 and below releases in the 4.27.x release train

Affected Platforms

The following EOS products are affected with the previously mentioned software versions.

- 720XP series
- 7050X3 series
- 7300X3 series

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

- Arista EOS Based products:
    - 710P Series
    - 722XP Series
    - 750X Series
    - 7010 Series
    - 7010X Series
    - 7020R Series
    - 7050X/X2 series
    - 7060X/X2/X4 series
    - 7130 series
    - 7150 series
    - 7160 series
    - 7170 series
    - 7250X series
    - 7260X/X3 series
    - 7280E/R/R2/R3 series
    - 7300X series
    - 7320X series
    - 7368X4 series
    - 7358X4 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

Dynamic NAT

A Security “drop” ACL that overlaps with the IP range of a dynamic NAT “permit” ACL is required for this vulnerability to be exploitable. Note that the packets that should have been dropped do not necessarily have to ingress on the port the NAT ACL is applied to, they just need the overlapping IP range. In this example, Ethernet1 can apply dynamic NAT to a packet, but Ethernet2 has the security ACL.

```
# Dynamic NAT configured on Ethernet1:
```

```
interface Ethernet1
   ip nat source dynamic access-list natAcl pool p1

ip nat pool p1 prefix-length 24
   range 20.1.1.5 20.1.1.5

ip access-list natAcl
   10 permit ip 192.0.0.0/8 any

# Security ACL configured on Ethernet2:

interface Ethernet2
   ip access-group securityAcl in

ip access-list securityAcl
   10 deny ip host 192.168.1.25 any
   20 permit ip any any
```

In the example above, the access list named ‘securityACL’ marks the packet from host 192.168.1.25 to be dropped when ingressing on port Ethernet2. But the packet also matches the NAT ACL 192.0.0.0/8 permit rule, and the packet is forwarded.

Static NAT

This security limitation also applies to static NAT. However, the configuration below can be classified as a mis-configuration (explicit “drop” security acl rule for host we want to NAT). The following configuration may make more sense to use different ip addresses for security ACL and static NAT.

```
# Static NAT configured on Ethernet1:

interface Ethernet1
   ip nat source static 192.168.1.125 20.1.1.5

# Security ACL configured on Ethernet2:

interface Ethernet2
   ip access-group securityAcl in

ip access-list securityAcl
   10 deny ip host 192.168.1.125 any
   20 permit ip any any
```

Static NAT configurations use the host address that needs to be translated using NAT. Unlike Dynamic NAT, static NAT use cases typically do not have port access-lists that are likely to overlap with the NAT access-list. For more information on configuring Static NAT see the configuration guide here.

Indications of Compromise

No evidence of compromise is detectable from internal logging.

Mitigation

The following configuration changes may be made in order to remedy the exploitation.

Configure a NAT “drop” ACL rule for each security ACL “drop” rule that should be applied to the interface that has NAT configured. This will prevent the packets from being translated at the expense of maintaining the configuration in two places.

Here we’ve added the deny rules from the Security ACL into the NAT ACL:

```
ip access-list natAcl
   10 deny ip host 192.168.1.25 any
   20 permit ip 192.0.0.0/8 any
```

For the final resolution, please refer to the resolution section which lists the details of the remediated software versions.

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience.

The fixed versions for the currently supported release trains are as follows:

- 4.24.10 and later releases in the 4.24.x train
- 4.25.9 and later releases in the 4.25.x train
- 4.26.6 and later releases in the 4.26.x train
- 4.27.4 and later releases in the 4.27.x train
- 4.28.0 and later releases in the 4.28.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 Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support