Date: August 9, 2024

Revision	Date	Changes
1.0	July 23, 2024	Initial release
1.1	August 9, 2024	Clarification of affected systems

The CVE-ID tracking this issue: CVE-2024-27891
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)
Common Weakness Enumeration: CWE-284: Improper Access Control
This vulnerability is being tracked by BUG 906098

Description

On affected platforms running Arista EOS with MACsec and egress ACLs configured on the same interfaces, the ACL policies may not be enforced for packets egressing on those ports. This can cause outgoing packets to incorrectly be allowed or denied.

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

- 4.32.0.1F and below releases in the 4.32.X train
- 4.31.2F and below releases in the 4.31.X train
- 4.30.6M and below releases in the 4.30.X train
- 4.29.7M and below releases in the 4.29.X train
- 4.28.10.1M and below releases in the 4.28.X train
- 4.27.2F and above releases in the 4.27.X train

Affected Platforms

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

- Arista EOS-based products:

    - 722XPM Series

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

- Arista EOS-based products:
    - 710 Series
    - 720D Series
    - 720XP 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/X6 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
    - AWE 5000 Series
    - AWE 7200R Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
- 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
- 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-2024-27891, multiple specific conditions must be met. Both MACsec and egress ACLs must be configured and active on the same interface as the minimum requirements for this issue to be exposed. Please review the following sections to identify if your organization is affected.

1. MACsec must be configured:

```
switch>show mac security status
Administrative State:     enabled
Active Profiles:          1
Data Delay Protection:    no
EAPoL Destination MAC:    0180.c200.0003
FIPS Mode:                no
Secured Interfaces:       54
License:                  enabled
```

Note: active profiles is not 0, and number of secured interfaces is not 0

If MACsec is not configured there is no exposure to this issue and the message will include 0 Active Profiles, and 0 Secured Interfaces.

```
switch>show mac security status
Administrative State:     enabled
Active Profiles:          0
Data Delay Protection:    no
EAPoL Destination MAC:    0180.c200.0003
FIPS Mode:                no
Secured Interfaces:       0
License:                  disabled (Hardware license not enabled)
```

2. Access Control Lists (ACLs) must be configured for outbound packets:

```
switch#show running-config | section access-list
ipv6 access-list testIp6Acl
ip access-list testIpAcl
mac access-list testMacAcl

switch#show running-config | section access-group
interface Ethernet1
   ip access-group testIpAcl out
```

The total number of ACLs configured must be any of the following:

1. More than 3 MAC ACLs, or
2. More than 7 IPv4 ACLs, or
3. More than 3 IPv6 ACLs

If for each ACL type in use, there are less than the above corresponding number configured there is no exposure to this issue.

If ACLs are not configured for outbound packets there is no exposure to this issue and the message will look like:

```
! Notice no output below, indicating no ACLs configured
! or notice ACLs are applied as “in” only.
switch#show running-config | section access-list
switch#
switch#show running-config | section access-group
interface Ethernet1
   ip access-group testIpAcl in
```

If no interfaces which have ACLs configured for outbound packets have MACsec configured, there is no exposure to this issue.

Note that interface types such as Vlan interfaces, or Port-Channel interfaces may have none, one or multiple physical interfaces.

To check for MACsec configuration, first resolve the access-group configured interfaces to a list of all Ethernet physical interfaces.

In the example below, there is an ACL applied to Port-Channel1 (Ethernet1, Ethernet5), Vlan613 (Ethernet2, Ethernet4) and Ethernet3. Therefore Ethernet1-5 should be checked to see if MACsec is enabled.

```
switch#show running-config | section access-group
interface Port-Channel1
   ipv6 access-group testIp6Acl out
interface Ethernet3
   ip access-group testIpAcl in
interface Vlan613
   ip access-group testIpAcl out

switch>show port-channel 1 brief
Port Channel Port-Channel1:
  Active Ports: Ethernet1 Ethernet5

switch>show vlan 613
VLAN  Name                             Status    Ports
----- -------------------------------- --------- -------------------------------
----------
613   VLAN0613                         active    Cpu, Et2, Et4

switch>show mac security interface Ethernet1-5
Interface       SCI                       Controlled Port      Key in
Use
Ethernet1       12:15:35:24:
c0:89::24193  True                 static SAK: Tx AN: 2
Ethernet2       00:00:00:00:00:00::0      False                None
Ethernet5       12:15:35:24:
c0:89::24193  True                 static SAK: Tx AN: 2
```

In the above example Ethernet1 and Ethernet5 have MACsec enabled.

In the example below, there are more than 3 IPv6 ACLs applied for outbound packets. All physical interfaces that are MACsec enabled, and have an IPv6 ACL applied for outbound packets, are exposed to this issue.

```
switch#show running-config | section access-group
```

```
interface Port-Channel1
   ipv6 access-group testIp6Acl out
interface Ethernet3
   ip access-group testIpAcl in
interface Ethernet45
   ipv6 access-group testIp6Acl2 out
interface Ethernet46
   ipv6 access-group testIp6Acl3 out
interface Ethernet47
   ipv6 access-group testIp6Acl4 out
interface Vlan613
   ip access-group testIpAcl out

switch>show port-channel 1 brief
Port Channel Port-Channel1:
  Active Ports: Ethernet1 Ethernet5

switch>show vlan 613
VLAN  Name                             Status    Ports
----- -------------------------------- --------- -------------------------------
----------
613   VLAN0613                         active    Cpu, Et2, Et4

switch>show mac security interface Ethernet1-$ | grep True
Ethernet1       12:15:35:24:c0:89::24193  True                static
SAK: Tx AN: 2
Ethernet2       12:15:35:24:c0:89::24193  True                static
SAK: Tx AN: 2
Ethernet5       12:15:35:24:c0:89::24193  True                static
SAK: Tx AN: 2
Ethernet45      12:15:35:24:c0:89::24193  True                static
SAK: Tx AN: 2
```

Interface	“Out” ACL	Minimum ACL count met	MACsec enabled	Affected
Et1	Yes	Yes	Yes	Yes
Et2	Yes	No (only one IPv4 ACL)	Yes	No
Et3	No	No (only one IPv4 ACL)	No	No

Interface	“Out” ACL	Minimum ACL count met	MACsec enabled	Affected
Et4	Yes	No (only one IPv4 ACL)	No	No
Et5	Yes	Yes	Yes	Yes
Et45	Yes	Yes	Yes	Yes
Et46	Yes	Yes	No	No
Et47	Yes	Yes	No	No

In the above example and table:

- Ethernet46 and Ethernet47 are not exposed to this issue, because they are not MACsec enabled.
- Ethernet2, Ethernet3, and Ethernet4 are not exposed to this issue because there is only one IPv4 ACL group, which is less than the required number to be exposed for that ACL type.
- Ethernet3 is also not affected because the ACL is for incoming packets.
- Ethernet1, Ethernet5, and Ethernet45 are affected by this issue because they meet the conditions required.

Indicators of Compromise

This vulnerability may lead to unexpected ACL behavior. Examples of misbehaving switches include:

- ACL drops for traffic which should be allowed
- No ACL drops for traffic which should be denied (traffic reaches peer devices unexpectedly)

Mitigation

The workaround is to disable MACsec on interfaces with outbound packet ACLs, or to use inbound packet ACLs where possible. Note that ingress ACLs might need to be applied to a different set of interfaces or to other devices in the network.

```
switch#configure
switch(config)#interface Ethernet1
switch(config-if-Et1)#no mac security profile
```

```
! or remove/replace the `out` ACL
! Note that you may wish to apply `in` ACLs to a different set of
! interfaces than `out` ACLs were applied to.

switch#configure
switch(config)#interface Ethernet1
switch(config-if-Et1)#mac access-group <ACL name> in
switch(config-if-Et1)#ip access-group <ACL name> in
switch(config-if-Et1)#ipv6 access-group <ACL name> in
switch(config-if-Et1)#no mac access-group out
switch(config-if-Et1)#no ip access-group out
switch(config-if-Et1)#no ipv6 access-group out
```

For more information about ACLs see EOS User Manual: ACLs and Route Maps.

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-2024-27891 has been fixed in the following releases:

- 4.32.1F and later releases in the 4.32.x train
- 4.31.3M and later releases in the 4.31.x train
- 4.30.7M and later releases in the 4.30.x train
- 4.29.8M and later releases in the 4.29.x train
- 4.28.11M and later releases in the 4.28.x train

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

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