Date: July 23, 2024

Revision	Date	Changes
1.0	July 23, 2024	Initial release

The CVE-ID tracking this issue: CVE-2024-6858
CVSSv3.1 Base Score: 6.5 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
Common Weakness Enumeration: CWE-287 Improper Authentication.
This vulnerability is being tracked by BUG 828435

Description

In Arista's EOS when in 802.1X mode, multi-auth unauthenticated hosts might be allowed access to a switch port if there exists an EAPOL capable device in the fallback VLAN.

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

- 4.31.1F and below releases in the 4.31.x train.
- 4.30.5M 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.

Affected Platforms

The following products **are** 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/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

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

- Arista EOS-based products:
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
    - CloudVision eXchange, virtual or physical appliance
    - AWE 5000 Series
    - AWE 7200 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
- 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)
- Arista NetVisor OS, Arista NetVisor UNUM, and Insight Analytics (Formerly Pluribus)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2024-6858, the following conditions must be met:

(1) dot1x should be configured on port as authenticator and port-control is auto mode and hostMode is multi-host. Please note the default host-mode is multi-host.

```
switch(config-if-et1)#show active
interface Ethernet1
   ……
   dot1x pae authenticator
   dot1x port-control auto
   dot1x host-mode multi-host
   ……
```

AND
(2) Fallback VLAN should be configured on port. Fallback VLAN can be configured in any of the following ways listed below;

(2-a) Global Configuration for unresponsive VLAN.

```
switch(config-dot1x)#show active
dot1x
   ……
   aaa unresponsive action traffic allow vlan <vlan-id>
   ……

OR

switch(config-dot1x)#show active
dot1x
   ……
   aaa unresponsive action traffic allow
   ……
```

OR
(2-b) Global Configuration for unresponsive phone VLAN.

```
switch(config-dot1x)#show active
dot1x
   ……
   aaa unresponsive phone action traffic allow
   ……
```

OR
(2-c) Global Configuration for guest VLAN.

```
switch(config-dot1x)#show active
dot1x
   ……
   eapol unresponsive action traffic allow vlan <vlan-id>
   ……
```

OR
(2-d) Authentication failure VLAN configured on port.

```
switch(config-if-et1)#show active
interface Ethernet1
   ……
   dot1x authentication failure action traffic allow vlan <vlan_id>
   ……
```

OR
(2-e) Unresponsive VLAN configured on port.

```
switch(config-if-et1)#show active
interface Ethernet1
   ……
   dot1x aaa unresponsive action traffic allow vlan <vlan_id>
   ……
```

OR
(2-f) Unresponsive phone VLAN configured on port.

```
switch(config-if-et1)#show active
interface Ethernet1
   ……
   dot1x aaa unresponsive phone action traffic allow
   ……
```

Indicators of Compromise

This vulnerability may allow network access to unauthenticated hosts.

The administrator can validate this by looking at the output of the dot1x configured interface.

Assume Ethernet1 is the dot1x configured interface, then look for the following where the MAC addresses do not match:

```
switch>show mac address-table dynamic interface ethernet 1
          Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type        Ports      Moves   Last Move
----    -----------       ----        -----      -----   ---------
2500    xxxx.xxxx.xxxx      DYNAMIC    Et2/1       1        0:00:13 ago
Total Mac Addresses for this criterion: 1

AND

switch>show dot1x hosts Ethernet 1
Port      Supplicant MAC Auth  State                    Fallback               VLAN
--------- -------------- ----- ---------------------- ---------------------- ----
Et2/1      yyyy.yyyy.yyyy   EAPOL FAILED                  NONE                 2600

OR

switch>show dot1x hosts Ethernet 1
Port      Supplicant MAC Auth  State                    Fallback               VLAN
--------- -------------- ----- ---------------------- ---------------------- ----
Et2/1     yyyy.yyyy.yyyy   EAPOL   AUTH-SERVER-TIMEOUT    NONE                 2600
```

In the above example the learned MAC address for an interface (output of "**show mac address-table dynamic interface ethernet 1**") does not match the list of authenticated supplicants (output of "show dot1x hosts Ethernet 1"). This shows that the mac address xxxx.xxxx.xxxx has bypassed 802.1x authentication.

Mitigation

This vulnerability arises when there is an EAPOL supplicant in any of the fallback VLAN's (i.e. auth-fail, unresponsive VLAN). If only unauthenticated EAPOL supplicants are expected the admin can change dot1x host-mode to single-host as indicated below.

```
switch(config-if-et1)#dot1x host-mode single-host
```

- Dot1x Host Mode

- Single Host Mode: Please note when once the 802.1X supplicant is authenticated on the port, ONLY the traffic coming from the supplicant's MAC is allowed through the port.
- Multi-Host Mode: Once the 802.1X supplicant is authenticated on the port, traffic coming from ANY source MAC is allowed through the port.
- Multi-Host authenticated Mode: Multiple 802.1X supplicants can be allowed and ONLY the traffic coming from all authenticated supplicant’s MAC is allowed through the port.

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-2024-6858 has been fixed in the following releases:

- 4.31.2F and later releases in the 4.31.x train.
- 4.30.6M and later releases in the 4.30.x train.
- 4.29.8M and later releases in the 4.29.x train.
- 4.28.11Mand later releases in the 4.28.x train.

Hotfix

No hotfix is available

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