Date: February 6, 2025

Revision	Date	Changes
1.0	January 14, 2025	Initial release
1.1	February 6, 2025	Updated EOS-Based Product Versions

The CVE-ID tracking this issue: CVE-2024-8000
CVSSv3.1 Base Score: 5.3 (CVSS:3.1/AV:A/AC:H/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 989881

Description

On affected platforms running Arista EOS with 802.1X configured, certain conditions may occur where a dynamic ACL is received from the AAA server resulting in only the first line of the ACL being installed after an Accelerated Software Upgrade (ASU) restart.

Note: supplicants with pending captive-portal authentication during ASU would be impacted with this bug.

The issue was discovered internally by Arista. Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.32.4M and below releases in the 4.32.x train
- 4.31.5M and below releases in the 4.31.x train
- 4.30.8M and below releases in the 4.30.x train

Affected Platforms

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

- Arista EOS-based products:
  - 710 Series
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series

    - 7010 Series
    - 7010X Series
    - 7170 Series
    - 7050X/X2/X3/X4 Series
    - 7060X/X2/X4/X5/X6 Series
    - 7260X/X3 Series
    - 7300X/X3 Series
    - 7320X Series
    - 7358X4 Series
    - 7368X4 Series
    - 7388X5 Series

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

- Arista EOS-based products:
    - 7020R Series
    - 7130 Series running EOS
    - 7160 Series
    - 7250X Series
    - 7280E/R/R2/R3 Series
    - 7500E/R/R2/R3 Series
    - 7800R3/R4 Series
    - 7700R4 Series
    - 7150 Series
    - AWE 5000 Series
    - CloudEOS
    - cEOS-lab
    - vEOS-lab
- Arista Wireless Access Points
- CloudVision CUE, virtual appliance or physical appliance
- CloudVision CUE cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- 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-2024-8000, the following three conditions must be met:

1. 802.1X must be configured.
2. The customer must have an external AAA server configured which sends a multi-line dynamic ACL.
3. ASU must have occurred (more information about the upgrade process can be found here at Upgrades and Downgrades - Arista). The version being upgraded from is an affected software version, and the version being upgraded to is an affected software version as listed above.

The below example shows an example of this issue before and after ASU:

```
switch#show dot1x hosts mac 0001.0203.0405 detail | json
{
    "supplicantMac": "00:01:02:03:04:05",
    "identity": "user3",
    "interface": "Ethernet3/47",
    "authMethod": "EAPOL",
    "authStage": "SUCCESS",
    "fallback": "NONE",
    "callingStationId": "00-01-02-03-04-05",
    "reauthBehavior": "DO-NOT-RE-AUTH",
    "reauthInterval": 0,
    "cacheConfTime": 0,
    "vlanId": "202",
    "accountingSessionId": "",
    "captivePortal": "",
    "captivePortalSource": "",
    "aristaWebAuth": "",
    "supplicantClass": "",
    "filterId": "",
    "framedIpAddress": "0.0.0.0",
    "framedIpAddrSource": "sourceNone",
    "nasFilterRules":  [
        "deny in ip from 10.1.0.0/16 to 20.1.0.0/16",
        "permit in ip from 11.0.0.0/8 to 12.0.0.0/8",
        "permit tcp any any eq 80",
        "permit tcp any any eq 443",
        “deny ip host 192.168.1.100"
    ],
    "sessionTimeout": 0,
    "terminationAction": "",
    "tunnelPrivateGroupId": "",
    "aristaPeriodicIdentity": "",
    "cachedAuthAtLinkDown": false,
    "reauthTimeoutSeen": false,
    "sessionCached": false,
    "detail_": true
}
```

The above example is before ASU. Note that the “nasFilterRules” has 5 rules in it.

When ASU is performed:

```
switch#show dot1x hosts mac 0001.0203.0405 detail | json
{
    "supplicantMac": "00:01:02:03:04:05",
    "identity": "user3",
    "interface": "Ethernet3/47",
    "authMethod": "EAPOL",
    "authStage": "SUCCESS",
    "fallback": "NONE",
    "callingStationId": "00-01-02-03-04-05",
    "reauthBehavior": "DO-NOT-RE-AUTH",
    "reauthInterval": 0,
    "cacheConfTime": 0,
    "vlanId": "202",
    "accountingSessionId": "",
    "captivePortal": "",
    "captivePortalSource": "",
    "aristaWebAuth": "",
    "supplicantClass": "",
    "filterId": "",
    "framedIpAddress": "0.0.0.0",
    "framedIpAddrSource": "sourceNone",
     "nasFilterRules": [
        "deny in ip from 10.1.0.0/16 to 20.1.0.0/16"
    ],
    "sessionTimeout": 0,
    "terminationAction": "",
    "tunnelPrivateGroupId": "",
    "aristaPeriodicIdentity": "",
    "cachedAuthAtLinkDown": false,
    "reauthTimeoutSeen": false,
    "sessionCached": false,
    "detail_": true
}
```

The above example is after ASU. Note the nasFilterRule is now only one line.

Note: This symptom is not present when a non-ASU upgrade (i.e. standard reboot) takes place.

Indicators of Compromise

This vulnerability may lead to unauthorized traffic flows if the ACL is not programmed correctly post ASU.

Another way to verify that there may be an issue is to check the output of the `**show ip access-lists**` command and verify that the Dynamic ACL is only one line as shown below.

```
switch#show ip access-lists
Phone ACL bypass: disabled
IP Access List 802.1x-3212953518080 [dynamic]
        10 deny ip 10.1.0.0/16 20.1.0.0/16

        Total rules configured: 1
```

Mitigation

The workaround is to re-authenticate each supplicant. This can be done by running the command “**dot1x re-authenticate**” on the interface post ASU. Alternatively, if the reauthentication timer is enabled, the ACL will be correctly reprogrammed once the timer has expired and re-authentication occurs.

```
switch(Ethernet 1)#dot1x re-authenticate
```

Alternatively, flapping the interface will trigger reauthentication of the supplicants and correct the ACL which is installed for each mac on that interface.

```
switch(Ethernet 1)#shut
switch(Ethernet 1)#no shut
```

In both cases mentioned, we can verify that reauth has been triggered by checking the output of `**show logging**` to show the supplicant has been successfully authenticated and `**show ip access-lists**` to verify the ACL is installed correctly.

```
switch(Ethernet 1)#show logging
Aug 24 07:12:05 switch Dot1x: DOT1X-6-SUPPLICANT_AUTHENTICATED: Supplicant with identity 00:01:02:03:04:05, MAC 0001.0203.0405 and dynamic VLAN None successfully authenticated on port Ethernet1.

switch#show ip access-lists
Phone ACL bypass: disabled
IP Access List 802.1x-3212953518000 [dynamic]
        10 deny ip 10.1.0.0/16 20.1.0.0/16
        20 permit ip from 11.0.0.0/8 to 12.0.0.0/8
        30 permit tcp any any eq 80
        40 permit tcp any any eq 443
        50 deny ip host 192.168.1.100

        Total rules configured: 5

switch#show dot1x hosts mac 0001.203.0405 detail | json
{
    "supplicantMac": "00:01:02:03:04:05",
    "identity": "user3",
    "interface": "Ethernet3/47",
    "authMethod": "EAPOL",
    "authStage": "SUCCESS",
    "fallback": "NONE",
    "callingStationId": "00:01:02:03:04:05",
    "reauthBehavior": "DO-NOT-RE-AUTH",
    "reauthInterval": 0,
    "cacheConfTime": 0,
    "vlanId": "202",
    "accountingSessionId": "",
    "captivePortal": "",
    "captivePortalSource": "",
    "aristaWebAuth": "",
    "supplicantClass": "",
    "filterId": "",
    "framedIpAddress": "0.0.0.0",
    "framedIpAddrSource": "sourceNone",
    "nasFilterRules": [
        "deny in ip from 10.1.0.0/16 to 20.1.0.0/16",
        "permit in ip from 11.0.0.0/8 to 12.0.0.0/8",
        "permit tcp any any eq 80",
        "permit tcp any any eq 443",
        “deny ip host 192.168.1.100"
    ],
    "sessionTimeout": 0,
    "terminationAction": "",
    "tunnelPrivateGroupId": "",
    "aristaPeriodicIdentity": "",
    "cachedAuthAtLinkDown": false,
    "reauthTimeoutSeen": false,
    "sessionCached": false,
    "detail_": true
}
```

In the above example the supplicant has been re-authenticated and the nasFilterRules shows 5 rules, as before.

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-2024-8000 has been fixed in the following releases:

- 4.33.0M and above
- 4.32.5M and above releases in the 4.32.x train
- 4.31.6M and above releases in the 4.31.x train
- 4.30.9M and above releases in the 4.30.x train

Hotfix

No hotfix exists 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

Contact information needed to open a new service request may be found at:

https://www.arista.com/en/support/customer-support