Date: May 21, 2024

Revision	Date	Changes
1.0	May 21, 2024	Initial release

The CVE-ID tracking this issue: CVE-2023-5502
CVSSv3.1 Base Score: 5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N)
Common Weakness Enumeration: CWE-287 Improper Access Control
This vulnerability is being tracked by BUG 862986

Description

On affected platforms running Arista EOS with 802.1x authentication configured on the access/trunk ports, and routing enabled on the access VLAN of the ports, a malicious supplicant may be able to bypass the requirement to perform 802.1x authentication.

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 from 4.17.0 onwards are affected including the following supported release trains:

- 4.31.0F and earlier releases in the 4.31.x train
- 4.30.4M and earlier releases in the 4.30.x train
- 4.29.6M and earlier releases in the 4.29.x train
- 4.28.8M and earlier releases in the 4.28.x train
- 4.27.11M and earlier releases in the 4.27.x train
- 4.26.11M and earlier releases in the 4.26.x train
- 4.25.11M and earlier releases in the 4.25.x train
- 4.24.11M and earlier releases in the 4.24.x train

Affected Platforms

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

- Arista EOS-based products:
    - 7020R Series
    - 7280R/R2 Series

  - 7500R/R2 Series
  - 7280E Series
    - Note that this product is EOL and there are no released versions of EOS which fix the issue.
  - 7500E Series
    - Note that this product is EOL and there are no released versions of EOS which fix the issue.

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

- Arista EOS-based products:
  - 710P/720XP/722XPM Series
  - 750X Series
  - 758X Series
  - 7010 and 7010X Series
  - 7050X/X2/X3/X4 Series
  - 7060X/X2/X4/X5/X6 Series
  - 7130 Series running EOS
  - 7150 Series
  - 7170 Series
  - 7250X Series
  - 7260X/X3 Series
  - 7280R3 Series
  - 7500R3 Series
  - 7800R3 Series
  - 7289R3 Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - AWE 5000 Series
- 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)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2023-5502, either of the following conditions must be met:

1. Dot1x authentication must be configured:

Global command to enable dot1x:

```
dot1x system-auth-control
interface Ethernet1
  dot1x pae authenticator
  dot1x port-control auto
  !! One of the two configuration lines below MUST be set
  dot1x host-mode single-host
  dot1x host-mode multi-host authenticated
interface Vlan100
  ip address 1.1.1.1/24
ip routing
```

2. There is a second vulnerable configuration where 802.1x is configured in any host mode with MBA as shown below:

```
dot1x system-auth-control
interface Ethernet1
  dot1x pae authenticator
  dot1x port-control auto
  dot1x mac based authentication
  !! One of the three configuration lines below MUST be set
  dot1x host-mode single-host
  dot1x host-mode multi-host authenticated
  dot1x host-mode multi-host
interface Vlan100
  ip address 1.1.1.1/24
ip routing
```

Indicators of Compromise

There is no indicators of compromise for this vulnerability

Mitigation

Mitigation of this vulnerability requires disabling dot1x.

Dot1x can be disabled globally using the following command

```
no dot1x system-auth-control
```

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-2023-5502 has been fixed in the following releases:

- 4.32.0F and later releases in the 4.32.x train
- 4.31.3M and later releases in the 4.31.x train
- 4.30.5M and later releases in the 4.30.x train
- 4.29.7M and later releases in the 4.29.x train

Hotfix

No hotfixes are 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

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