Date: July 20th, 2022

Revision	Date	Changes
1.2	July 20th 2022	Upload the hotfix for 4.23 train
1.1	May 13rd 2022	Update fixed release info
1.0	April 26th 2022	Initial release

CVE-2022-0778

- CVSSv3.1 Base Score: 7.5(CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
- CWE: CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')
- This vulnerability is being tracked by BUG674519(EOS) and BUG680261(MOS)

Description

This advisory documents the impact of a publicly disclosed vulnerability in OpenSSL on Arista products.

There exists a vulnerability in OpenSSL versions 1.0.2, 1.1.1, and 3.0 in which a certificate containing invalid elliptic curve parameters can cause Denial-of-Service (DoS) to the application by triggering an infinite loop.

Arista Engineering and Security teams have evaluated the impact of the vulnerability and are diligently working on the fixes. The fixed release versions for all products will be updated in this advisory as soon as possible.

The vulnerability was reported externally by upstream and Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

The following products are affected by CVE-2022-0778:

- Arista EOS-based products
    - 4.27.3 and below releases in the 4.27.x train
    - 4.26.5 and below releases in the 4.26.x train

    - 4.25.8 and below releases in the 4.25.x train
    - 4.24.9 and below release in the 4.24.x train
    - 4.23.11 and below release in the 4.23.x train
    - 4.22.x train
- Arista 7130 Systems running MOS
    - MOS-0.10.0 to MOS-0.36.2

The following products are NOT affected by CVE-2022-0778:

- Arista Wireless Access Points
- CloudVision as-a-Service
- CloudVision WiFi cloud service delivery (patch already applied)

The following products have low impact by CVE-2022-0778:

The products mentioned below do have the vulnerable openSSL version installed, but they are usually running in the protected internal network with no access to external routed traffic. Therefore the impact of CVE-2022-0778 is considered low risk to those products.

- CloudVision Portal, virtual appliance or physical appliance
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- CloudVision WiFi, virtual appliance or physical appliance

The NDR/Awake products do have the vulnerable openSSL version installed, but the TLS sessions are established with trusted vendor networks selected and configured by the Awake team with continuous monitoring . Therefore the impact of CVE-2022-0778 is considered low risk.

- Awake Security Platform

Note: even though the above products are considered low risk, the development teams are actively working on the patch to maintenance releases. The fixed version info will be updated in the advisory soon.

Mitigation

The following configuration changes may be made to mitigate the exploitation of the listed vulnerability.

Arista EOS-based products

Control plane ACL and TLS server service ACLs can be used to mitigate the vulnerability by installing ACL rules to restrict traffic only from trusted sources.

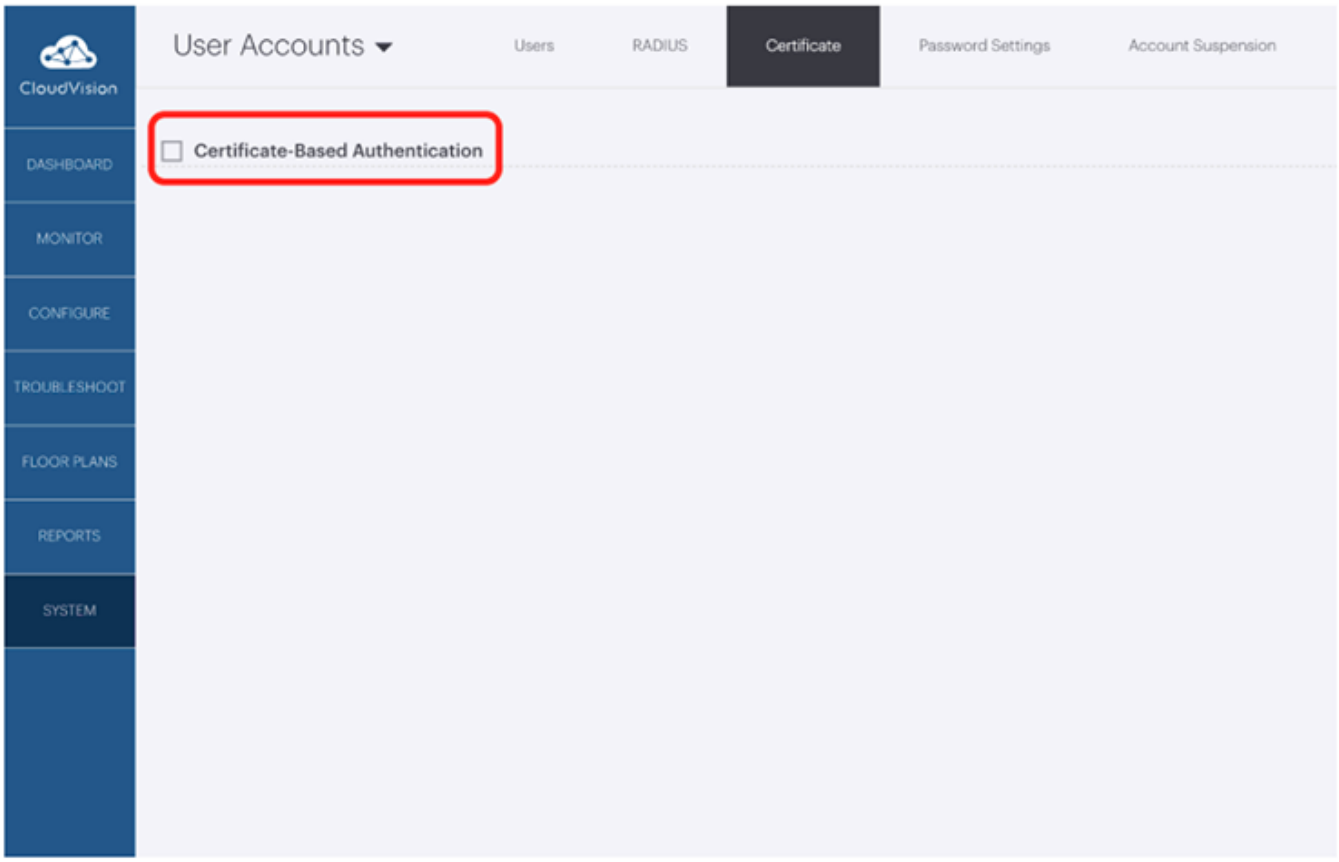
The detailed explanation and instruction of how to configure or modify ACL can be found in the

manual. Here is a simple example of using service ACL to restrict traffic to protocol HTTP/S from trusted users in the subnet of 192.168.100.0/24 via eAPI.

```
management http-server
   protocol http
   !
   vrf default
      ip access-group httpAcl in
<-------OUTPUT OMITTED FROM EXAMPLE-------->
!
ip access-list httpAcl
   10 permit ip 192.168.100.0/24 any
```

CloudVision WiFi, virtual appliance or physical appliance

The user certificate-based authentication is disabled by default, please check the Certificate page on the CloudVision UI to make sure the Certificate-Based Authentication setting box is unchecked.



There are no mitigation procedures available for the remaining affected products.

Resolution

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

Arista EOS-based products

This vulnerability has been fixed in the following EOS version:

- 4.27.4 and later releases in the 4.27.x train
- 4.26.6 and later releases in the 4.26.x train
- 4.25.9 and later releases in the 4.25.x train
- 4.24.10 and later release in the 4.24.x train
- 4.23.12 and later release in the 4.23.x train

Hotfix

For an immediate remediation until EOS can be upgraded, the following hotfixes are available.

The hotfix can be installed as an EOS extension and is applicable across all affected EOS versions.

The SWIX installation is hitless with SuperServer and Aaa agents being restarted. The existing session should not get interrupted but it's suggested to re-login after the hotfix installation.

- Release versions: 4.24.0 and later affected releases
    - Hotfix SWIX URL: SecurityAdvisory0075Hotfix.swix
    - Hotfix SWIX hash: (SHA-512)9fc1a8257e1a1c74e34af51ae2e0b270c0ab5d0fc391239a5b7f4d2d6bcd097010343cd447834105aca68c4fb273002a1cc9a1a3e0e3dc5ef63858abd2575474
- Release versions: 4.23.0-4.23.11
    - Hotfix SWIX URL: SecurityAdvisory0075Hotfix_4.23.swix
    - Hotfix SWIX hash: (SHA-512)4c6adb4f1323185f137dc3327cb4cb5e56d36bbeedf4667eccdcb8c842c7957ef979bcdc12c05e8eeefec2c39c55527a02194feb453dd01cf9a78b4fe9ddbfc6

For instructions on installation and verification of the hotfix patch, refer to the “managing eos extensions” section in the EOS User Manual. Ensure that the patch is made persistent across reboots by running the command “**copy installed-extensions boot-extensions**”.

Arista 7130 Systems running MOS

This vulnerability has been fixed in the following MOS version:

- MOS-0.36.3 and later MOS releases

Hotfix

A hotfix has been implemented as a MOS extension, which can be downloaded from the following link.

- Hotfix URL: hotfix-sa75.swix
- Hotfix change log: hotfix-3.0.0-changelog.txt
- Hotfix hash: (SHA-512)ca93095b167e722f179d89f8f0146376281930e2b517bf1d9d56a0d840741b12192df4f14ba99e89e431b71877e0e81ece03954ba116a637732ced26ee52ee6b

The above hotfix SWIX is applicable to the following releases:

- MOS-0.27.0 and later affected releases

Note: for customers using releases older than MOS-0.27.0, please install the following RPMs. The RPMs must be installed in the following order:

- libcrypto: libcrypto1.1-1.1.1n-hotfix_sa75.core2_64.rpm
- libssl: libssl1.1-1.1.1n-hotfix_sa75.core2_64.rpm
- openssl: openssl-1.1.1n-hotfix_sa75.core2_64.rpm
- openssl-bin: openssl-bin-1.1.1n-hotfix_sa75.core2_64.rpm
- hotfix-sa75: hotfix-sa75-3.0.0-1.8.core2_64.rpm

To install the hotfix, follow these instructions:

- Copy the SWIX or RPMs to the device and install as an application
- App install instructions available on EOS Central here and in Section 5.7 (Application Commands) of the user guide available on the release page.
- Verification of install can be done by checking the syslogs or the applications list in the output of ‘show version’
- The hotfix will remain installed until explicitly removed, though it will not have any effect on the remediated releases. To remove the application, run the command: ‘**remove app hotfix-sa75**’ at the config prompt.

References

- https://nvd.nist.gov/vuln/detail/CVE-2022-0778
- https://access.redhat.com/security/cve/cve-2022-0778
- https://www.openssl.org/news/secadv/20220315.txt

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