Date: February 2nd, 2022

Version: 1.0

Revision	Date	Changes
1.0	February 2nd, 2022	Initial Release

The CVE-ID tracking this issue: CVE-2021-28503
CVSSv3.1 Base Score: 7.4(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H)
The internal bug tracking this issue: BUG606686

Description

This advisory documents the impact of an internally found vulnerability in Arista's EOS software.

The impact of this vulnerability is that eAPI may skip re-evaluating user credentials when certificate based authentication is used, which allows remote attackers to access the device via eAPI.

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:

- 4.26.2 and below releases in the 4.26.x train
- 4.25.5 and below releases in the 4.25.x train
- 4.24.7 and below releases in the 4.24.x train
- 4.23.9 and below releases in the 4.23.x train
- All releases in 4.22.x train

Affected Platforms

This is a platform-independent vulnerability and affects all systems running EOS (including CloudEOS and vEOS-lab) with the versions identified above.

The following products are **not** affected:

- 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

- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Awake Security Platform

Required Configuration for Exploitation

EAPI is enabled with user certificate authentication configuration.

```
management security
   ssl profile profileEAPI
      certificate httpServer.cert key httpServer.key
      trust certificate user.cert
      trust certificate ca.cert

management api http-commands
   protocol https ssl profile profileEAPI
   no shutdown
```

Indicators of Compromise

Unexpected login activities from certificate based authentication username can be used to indicate the exploitation of this vulnerability.

Check accounting logs on AAA server

If EXEC accounting is configured, the accounting logs on AAA server for multiple logins at the same time by the same certificate based authentication username can be used to indicate the exploitation of this vulnerability.

Check eAPI request activities on device

The eAPI request activities submitted by the certificate based authentication username in the following show command can be used to indicate the exploitation of this vulnerability.

For example, a user certificate generated with username “alice” is configured to eAPI SSL profile, then check the request count number and last request time of user “alice” to make sure the output is expected.

```
switch#show management api http-commands
Enabled:            Yes
HTTPS server:       running, set to use port 443
HTTP server:        shutdown, set to use port 80
Local HTTP server:  shutdown, no authentication, set to use port 8080
```

```
Unix Socket server: shutdown, no authentication
VRFs:               default
Hits:               39
Last hit:           493 seconds ago
Bytes in:           38477
Bytes out:          13750
Requests:           38
Commands:           186
Duration:           94.179 seconds
SSL Profile:        profileEAPI, valid
FIPS Mode:          No
QoS DSCP:           0
Log Level:          none
CSP Frame Ancestor: None
TLS Protocols:      1.0 1.1 1.2
   User        Requests       Bytes in       Bytes out    Last hit
----------- -------------- -------------- --------------- ---------------
   admin       29             36991          8308         493 seconds ago
   alice       9              1486           5442         497 seconds ago

URLs
----------------------------------------
Management1 : https://:443
```

Mitigation

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

Disallowing user certificate authentication via eAPI can be used to mitigate the vulnerability.

```
switch(config)#management security
switch(config-mgmt-security)#ssl profile profileEAPI
switch(config-mgmt-sec-ssl-profile-profileEAPI)#no trust certificate user.cert
switch(config-mgmt-sec-ssl-profile-profileEAPI)#exit
```

Resolution

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

The vulnerability is fixed in the following EOS versions:

- 4.26.3 and later releases in the 4.26.x train
- 4.25.6 and later releases in the 4.25.x train
- 4.24.8 and later releases in the 4.24.x train
- 4.23.10 and later releases in the 4.24.x train

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

Hotfix

The hotfix can be installed as an EOS extension and is applicable across all affected EOS versions. The hotfix SWIX installation is hitless with CapiApp agent being restarted.

- Hotfix SWIX URL: SecurityAdvisoryShastaHotfix.swix
- Hotfix SWIX hash: (SHA-512)d4f5221f8d5f3cceb74a61e733c570f326a5ade4d845f58929bd0902932218d8c9065675198c515cc194bcb2eaa8bc23ffe7136e91eedf478d23a1a0154138f9

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*'.

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