Date: August 20th, 2021

Version: 1.0

Revision	Date	Changes
1.0	August 20th, 2021	Initial Release

The CVE-ID tracking this issue: CVE-2021-28498
CVSSv3.1 Base Score: 8.7 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:H)

The CVE-ID tracking this issue: CVE-2021-28499
CVSSv3.1 Base Score: 6.3 (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L)

Description

This advisory documents the impact of two internally found vulnerabilities in Arista's MOS (Metamako Operating System) software which is supported on the 7130 product line. The vulnerabilities involve user account passwords (CVE-2021-28499) or enable passwords (CVE-2021-28498) set in clear text could result in unprivileged users getting complete access to the systems.

Both issues were discovered internally and Arista is not aware of any malicious uses of this issue in customer networks.

Vulnerability Assessment

Affected Software

MOS

- MOS-0.13 and post releases in the MOS-0.1x train
- MOS-0.26.6 and prior releases in the MOS-0.2x train
- MOS-0.31.1 and prior releases in the MOS-0.3x train

Affected Platforms

The following products are affected by this vulnerability:

- Arista 7130 Systems running MOS

The following products are **not** affected:

- Arista EOS-based products
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Arista Wireless Access Points

- CloudVision Wi-Fi (on-premise and cloud service delivery)
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- Awake Security Platform

Symptoms

To check the version of MOS running on the system, use the following commands

```
Switch#show version
Device: Metamako MetaConnect 96 with E-Series
SKU: DCS-7130-96E
Serial number: C96E-A7-36803-2

Software image version: 0.26.5

<output omitted for brevity>
```

In the above example, as the Switch is running 0.26.5, it is exposed to the vulnerability. During the creation of local user accounts, if the option of ‘0’ or ‘plaintext’ was used like shown in the example below, the password will be stored in clear text in the running configuration and any subsequent outputs that use the running configuration like the ‘show tech-support’ command. This has been addressed in the fixed releases noted in the ‘Resolution’ section of this advisory.

```
switch(conf)#username test secret 0 opensesame
```

Mitigation

A simple configuration change that aligns with security best practice can be used as an immediate mitigation. Follow the steps below:

1. Change the password for user accounts and the enable password and set them with SHA512 option.

```
switch# config
switch(conf)#username bil
l privilege 2 secret sha512
$6$VclX0m78qOPNJLBD$g.B61.fmqMxfDlkMC1waI1BQ9fqFD66mxdlZwbaefIdgoArFr5HV3qHOgb
```

```
SZkUXrpBztj6GE.61jxFDsO/45b
```

In the above example, the highlighted portion of the output is the encrypted string.

2. Clear device log messages

```
switch# bash sudo rm -f /var/log/messages*
```

3. Clear CLI history

```
switch# clear history
```

For the final resolution, please refer to the next section which lists the details of the remediated software versions.

Resolution

These vulnerabilities are being tracked by the following bug IDs - BUG567393 (CVE-2021-28499) and BUG567395 (CVE-2021-28498). The recommended resolution is to upgrade to a remediated MOS version during a maintenance window or to install the hotfix.

This vulnerability has been fixed in the following MOS version:

- MOS-0.26.7
- MOS-0.32.0

A hotfix has been implemented as an extension, which can be downloaded from the following link. Note that in addition to patches for these two vulnerabilities described in this security advisory 64, this hotfix also contains patches for vulnerabilities covered under security advisories 65 and 66.

- Hotfix URL: SecurityAdvisory64-67-Hotfix-mos-1818-2.0.0-1.11.core2_64.rpm
- Hotfix change log: hotfix-2.0.0-changelog.txt
- Hotfix hash: (SHA-256)af653e6306d540c54519f33a65352fd29baddf0009b47326cc313aa950811f95

The above hotfix is applicable to the following releases:

- MOS-0.26.6 and below releases in the MOS-0.26.x train
- MOS-0.31.1 and below releases in the MOS-0.3x train

To install the hotfix, follow these instructions:

- Copy the RPM to the device and install as an application
- App install instructions available on EOS Central here and also 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 mos-1818-2.0.0**’ at the config prompt

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