Date: August 20th, 2021

Version: 1.0

Revision	Date	Changes
1.0	August 20th, 2021	Initial Release

The CVE-ID tracking this issue: CVE-2021-28495
CVSSv3.1 Base Score: 7.2 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L)

Description

This advisory documents the impact of an internally found vulnerability in Arista's MOS (Metamako Operating System) software which is supported on the 7130 product line. Under certain conditions, user authentication can be bypassed when API access is enabled via the JSON-RPC APIs.

This issue was 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.

Check if API access is enabled:

```
Switch#show api status
JSON API server status: Started
```

In the above example, the output of the command shows that the API server is in the ‘Started’ state (highlighted) and hence enabled. This setting is required for the device to be vulnerable.

Mitigation

API access to the affected systems can be disabled by using the following commands. However, note that this will break any automation that relies on API access to the system and should be used only if API access is not required for managing the system.

```
Switch#conf
Switch(config)#management api
Switch(config-mgmt-api)#shutdown
Switch(config-mgmt-api)#show api status
JSON API server status: Stopped
```

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

Resolution

This vulnerability is being tracked by BUG567400. The recommended resolution is to upgrade to a remediated MOS version during a maintenance window.

This vulnerability has been fixed in the following MOS version:

- MOS-0.26.7 and later releases
- MOS-0.32.0 and later releases

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

- 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

The above hotfix is applicable to the following releases:

- 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