Date: August 20th, 2021

Version: 1.0

Revision	Date	Changes
1.0	August 20th, 2021	Initial Release

The CVE-ID tracking this issue: CVE-2021-28494
CVSSv3.1 Base Score: 9.6(CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:H)

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. The effect of this vulnerability is that, under certain conditions, authentication is bypassed by unprivileged users who are accessing the Web UI.

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-0.34.0 and prior releases

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

Check if the installed software version falls under the list specified in the “Affected Software” section:

```
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.

Mitigation

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

```
Switch#conf
Switch(config)#management http
Switch(conf-mgmt-http)#shutdown
Switch(conf-mgmt-http)#show http status
       HTTP server status: Stopped
       HTTP protocol: Secure
       HTTP server port: 443
```

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 BUG567401. 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-0.35.0

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