Date: August 20th, 2021

Version: 1.0

Revision	Date	Changes
1.0	August 20th, 2021	Initial Release

The CVE-ID tracking this issue: CVE-2021-28493
CVSSv3.1 Base Score: 8.4 (CVSS:3.1/AV:L/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, a user may be able to execute commands despite not having the privileges to do so.

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-0.32.0 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

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

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

The following workarounds may be leveraged as mitigation:

1. Change home directory permission for privileged groups

```
switch# bash chown -R $USER:admins $HOME
```

2. Change .bashrc to limit permissions

```
switch# bash chmod -R u-w,g-X $HOME
```

To make the mitigation persistent across reboots, please add the steps above in startup-config with the command below:

```
switch# bash echo $'bash find /home/* -maxdepth 0 -type d -exec sh -c \'chown -R \"$(
basename ):admins\" \"\" && chmod -R u-w,g-X \"\"\' \;' >> /mnt/flash/startup-config
```

Resolution

This vulnerability is being tracked by BUG567402. The recommended resolution is to upgrade to a remediated MOS version during a maintenance window.

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.

This vulnerability has been fixed in the following MOS version:

- MOS-0.33.0

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

Copyright 2026 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista, the Arista logo and EOS are trademarks of Arista Networks. Other product or service names may be trademarks or service marks of others.