Date: December 5, 2023

Revision	Date	Changes
1.0	December 5, 2023	Initial release

The CVE-ID tracking this issue: CVE-2023-24547
CVSSv3.1 Base Score: 5.9 (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H)
Common Weakness Enumeration: CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer
This vulnerability is being tracked by BUG868319, BUG873034, MOS-2222, MOS-2255.

Description

On affected platforms running Arista MOS, the configuration of a BGP password will cause the password to be logged in clear text that can be revealed in local logs or remote logging servers by authenticated users, as well as appear in clear text in the device’s running config. This could result in unauthorized route announcements from malicious peers or cause traffic loss.

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 Versions

- MOS-0.13.0 onwards

Affected Platforms

The following products **are** affected by this vulnerability:

- Arista 7130 Systems running MOS
- Pre-Arista labeled devices (Metamako)

The following product versions and platforms **are not** affected by this vulnerability:

- Arista EOS-based products:
  - 720D Series
  - 720XP/722XPM Series
  - 750X Series
  - 7010 Series

  - 7010X Series
  - 7020R Series
  - 7130 Series running EOS
  - 7150 Series
  - 7160 Series
  - 7170 Series
  - 7050X/X2/X3/X4 Series
  - 7060X/X2/X4/X5 Series
  - 7250X Series
  - 7260X/X3 Series
  - 7280E/R/R2/R3 Series
  - 7300X/X3 Series
  - 7320X Series
  - 7358X4 Series
  - 7368X4 Series
  - 7388X5 Series
  - 7500E/R/R2/R3 Series
  - 7800R3 Series
  - CloudEOS
  - cEOS-lab
  - vEOS-lab
  - AWE 5000 Series
- Arista Wireless Access Points
- CloudVision WiFi, virtual appliance or physical appliance
- CloudVision WiFi cloud service delivery
- CloudVision eXchange, virtual or physical appliance
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision AGNI
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)
- Arista Network Detection and Response (NDR) Security Platform (Formerly Awake NDR)
- Arista Edge Threat Management - Arista NG Firewall and Arista Micro Edge (Formerly Untangle)

Required Configuration for Exploitation

In order to be vulnerable to CVE-2023-24547 the following condition must be met:

A BGP password must be configured and be in plain text. An example of this is shown below:

```
switch>show running-config bgp
router bgp 65000
   neighbor 192.0.2.1 remote-as 66000
   neighbor 192.0.2.1 password pA$$w0rd
```

If a BGP password is not configured there is no exposure to this issue.

Indicators of Compromise

No indicators of compromise exist.

Mitigation

No mitigation exists.

Resolution

The recommended resolution is to upgrade to a remediated software version at your earliest convenience. Arista recommends customers move to the latest version of each release that contains all the fixes listed below. For more information about upgrading see the MOS User Guide: Updating

CVE-2023-24547 has been fixed in the following releases:

- MOS-0.36.10 and later releases in the MOS-0.36.x train
- MOS-0.39.4 and later releases in the MOS-0.39.x train

Because this issue would cause the password to be saved in logs and remote AAA servers it is recommended to also rotate the BGP password, if possible. Upon upgrading to a new release, the BGP password will be obfuscated with the type-7 algorithm as shown below:

```
switch>show running-config bgp
router bgp 65000
   neighbor 192.0.2.1 remote-as 66000
   neighbor 192.0.2.1 password key 7 00143242404C5B140B
```

Hotfix

The following hotfix can be applied to remediate CVE-2023-24547. The hotfix only applies to the releases listed below and no other releases. All other versions require upgrading to a release containing the fix (as listed above):

- MOS-0.39.3 and below releases in the MOS-0.39.x train
- MOS-0.38.1 and below releases in the MOS-0.38.x train
- MOS-0.37.1 and below releases in the MOS-0.37.x train
- MOS-0.36.9 and below releases in the MOS-0.36.x train

- MOS-0.35.3 and below releases in the MOS-0.35.x train
- MOS-0.34.0 in the MOS-0.34.x train

Please note that the only MOS release trains currently under maintenance support are MOS-0.39.x and MOS-0.36.x. The hotfix working for other releases should not be treated as evidence that these releases continue to be supported. For security it is important to ensure supported releases are used.

```
Version: 1.0
URL: hotfix-cve-2023-24547-4.0.0-1.14.core2_64.rpm
SWIX hash:(SHA512)
168b2ee3deb8d4a3151b9c24936ff9d6523557b366ceffc98e57e8bf80638997
```

For instructions on installation and verification of the hotfix patch, refer to the "How to Install an Application" Guide.

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
Contact information needed to open a new service request may be found at:
https://www.arista.com/en/support/customer-support