Date: June 3, 2020

Version: 1.0

Revision	Date	Changes
1.0	June 3, 2020	Initial Release

The CVE-ID tracking this issue: CVE-2020-11622
CVSSv3.1 Base Score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Description:

This security advisory documents the exposure of Arista's products to a security vulnerability in CloudEOS/vEOS Router. The vulnerability is specific to CloudEOS VM / vEOS Router software, and does not impact EOS running on physical switches, routers, or any other Arista products. This vulnerability can lead to an impact on traffic forwarding if a specific malformed TCP packet is delivered over the data plane.

The vulnerability is in Arista's CloudEOS VM / vEOS Router code in a scenario where TCP MSS options are configured.

Symptoms

An attack due to this vulnerability could result in an impact on data plane traffic forwarding owing to a specific corrupted TCP packet. There might not be any logging of the exploitation but the vulnerability is only exploitable when 'tcp mss ceiling' is configured on the tunnel.

To verify if exploitation is possible, check to see if **tcp mss ceiling** is applied to any interface, as per the example below. If **tcp mss ceiling** is not present, this vulnerability cannot affect the interface.

Example Vulnerable Interface:

```
interface Tunnel2
   description usa  guest tunnel
   vrf guest
   ip address 192.111.100.xx/30
   tcp mss ceiling ipv4 1300
```

Follow these steps to identify if you are affected by this vulnerability:

Validate the impact on data plane traffic by checking the packet counter on all active ports from the bash shell.

```
#bash /usr/share/bess/bessctl/bessctl 'show port'
```

When running the command, it is possible for the command to hang. If the command does not return a response in 30 seconds, the vulnerability has been exploited. If the command returns, note the packet counts for all active ports and run the command again after an additional 30 seconds. On running the command again, if either packet count, RX or TX, is the same on any active port the vulnerability has been exploited.

The below example shows a successful output:

```
PMD_et1      Driver PMDPort    HWaddr 00:0d:3a:9f:f4:55
               Speed 40,000Mbps  Link UP    Duplex FULL  Autoneg ON
       Inc/RX  packets: 385,929,812         bytes: 294,560,170,130
               dropped: 0
       Out/TX  packets: 245,969,566         bytes: 129,526,293,605
               dropped: 0
```

If the packet count increases, the system has not been exploited by the vulnerability.

Vulnerability Assessment

Affected Software

- CloudEOS VM /vEOS Router
  - 4.23.2M and below releases in the 4.23.x train
  - 4.22.4M and below releases in the 4.22.x train
  - 4.21.3M to 4.21.9M releases in the 4.21.x train
  - Special releases:
    - 4.21.3FX-7368.*, 4.21.4-FCRFX.*, 4.21.4.1, 4.21.7.1, 4.22.2.0.1, 4.22.2.2.1, 4.22.3.1, 4.23.2.1

Affected Platforms

- This vulnerability affects systems running CloudEOS VM / vEOS Router with the versions identified above
- The following products are **not affected**:
  - EOS running on Arista switching platforms
  - Arista Wireless Access Points
  - CloudVision virtual and physical appliances
  - CloudEOS Container, that runs in Kubernetes on-premises clusters
  - Arista 7130 Systems running MOS
  - Big Switch Nodes for BCF and BMF (Arista CCF and DMF)

Mitigation

To recover an impacted system from such a state, a workaround is to restart the SFE agent.

```
(config)#agent sfe terminate
```

Restarting the SFE agent will result in the dataplane being unable to forward packets for up to 3 minutes.

As a resolution against this vulnerability, refer to the section entitled “Resolution” for remediated CloudEOS VM / vEOS Router software versions and hotfix.

Resolution

This vulnerability is tracked by Bug 471392. To safeguard against this vulnerability, the recommended course of action is to install the provided hotfix or upgrade to a remediated CloudEOS VM / vEOS Router version.

The vulnerability is fixed in the following CloudEOS VM / vEOS Router versions:

- 4.24.1F and later releases
- 4.23.3M and later releases
- 4.22.5M and later releases
- 4.21.11M and later releases
- Special releases: 4.24.0FX and later

If you are unable to upgrade right away, the fix is available as a hotfix and should be applied to safeguard against this vulnerability.

The hotfix can be installed as an extension and is supported on all affected CloudEOS VM / vEOS Router versions. The hotfix installation will restart the forwarding process and reestablish data plane forwarding.

For instructions on installation and verification of extensions, refer to this section in the EOS User Manual: https://www.arista.com/en/um-eos/eos-section-6-7-managing-eos-extensions. Ensure that the extension is made persistent across reboots by copying the installed-extensions to boot-extensions.

- Patch file download URL: SecurityAdvisory0049Hotfix.swix
- Sha512sum: 4bc456390bd950a4f25961e66163f68cc350c495ee94fca6e7479b09036635f55a4a4897ae7d9aa3c43916240e8306824124d20dd0c878b0deb7135b432eff04

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