Date: May 2nd, 2018

Version: 1.0

Revision	Date	Changes
1.0	May 2nd, 2018	Initial Release

Affected Platforms: All EOS platforms

Affected Software Version: 4.20.1FX-Virtual-Router

The CVE-ID tracking this issue is CVE-2017-18017

CVSS v3: 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Impact:

This advisory is to document a security vulnerability that affects Arista products.

The tcpmss_mangle_packet function in the Linux kernel allows potential remote attackers to crash the vEOS instance and possibly run arbitrary code when iptables rules with TCPMSS action are configured because of a use-after-free in tcpmss_mangle_packet. Arista's vEOS router software is susceptible to this vulnerability.

Mitigation:

BUG 212726 tracks this vulnerability. A fix for this issue will be available in a future release.

Note: This vulnerability can be exploited only when using Tunnelintf configuration, disabling this wherever possible can mitigate this attack.

Resolution: It is recommended to install the patch provided on affected versions of EOS

Patch file download URL:

SecurityAdvisory0034Hotfix.swix

Sha256 sum is:

[admin@switch flash]$ sha256sum SecurityAdvisory0034Hotfix.swix

a261a32b9d927aa28d9859125088b5d4dcd4b2a81849098c6b0f67170920f88b SecurityAdvisory0034Hotfix.swix

Note:

- This hotfix can be installed on the affected version 4.20.1FX-Virtual-Router
- A reload of the switch is not required for the patch to take effect
- The configured tunnels may not work properly for up to 5 seconds while the patch is being applied.

Instructions to install the patch:

1. Download the patch file and copy the file to the extension partition of the switch using one of the supported file transfer protocols:

```
switch#copy scp://10.10.0.1/SecurityAdvisory0034Hotfix.swix exten
sion:
switch#verify /sha256 extension:SecurityAdvisory0034Hotfix.swix
```

2. Verify that the checksum value returned by the above command matches the provided SHA256 checksum for the file
3. Install the patch using the extension command. The patch takes effect immediately at the time of installation.

```
switch#extension SecurityAdvisory0034Hotfix.swix
```

4. Verify that the patch is installed using the following commands:

```
switch#show extensions
Name                                    Version/Release      Status
     Extension
----------------------------------- -------------------- -------
---- ---------
SecurityAdvisory0034Hotfix.swix         1.0.0/1.fc18         A, NI
     1
awsha.rpm                               0.1.1/1              A, I
     1
awslogs.swix
```

5. Make the patch persistent across reloads. This ensures that the patch is installed as part of the boot-sequence. The patch will not install on EOS versions with the security fix.

```
switch#copy installed-extensions boot-extensions
switch#show boot-extensions
SecurityAdvisory0034Hotfix.swix
```

References:

https://nvd.nist.gov/vuln/detail/CVE-2017-18017

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