Date: March 1st, 2018

Version: 1.0

Revision	Date	Changes
1.0	March 1st, 2018	Initial Release

Affected Platforms: All EOS platforms

Affected Software Version: This issue was introduced in EOS-4.19.0F release.

The CVE-ID tracking this issue is CVE-2018-5255

CVSS v3: 5.8 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L

Impact:

This advisory is to document a security vulnerability that affects Arista products. The switch's Mlag agent may restart unexpectedly when processing malformed UDP packets on a specific UDP port destined to the switch's ip address. Such malformed UDP packets with specific port numbers are not expected to be received in typical production environments and have to be crafted and sent with the malformed values by a malicious user.

BUG 234146 tracks the potential crash that can be caused by this vulnerability.

The backtrace of the crash file will have the following information if the Mlag agent restarted because of this vulnerability.

.... File "/usr/lib/python2.7/site-packages/MlagShared.py", line 118, in validateHeartbeatPkt struct.unpack(UDPHEARTBEAT_HDR_FORMAT, hdr)......

Mitigation:

BUG 234146 tracks this vulnerability. A fix for this issue is available from SW versions 4.19.4M , 4.20.2F onwards.

Resolution: It is recommended to upgrade EOS to versions with the fix or install the patch provided on affected versions of EOS

Patch file download URL:

CVE-2018-5255-4-19-hotfix.swix for SW versions 4.19.0F, 4.19.1F, 4.19.2F, 4.19.2.1F, 4.19.2.2F, 4.19.3F

CVE-2018-5255-4-20-hotfix.swix for SW versions 4.20.1F

Sha256 sum is:

[admin@switch flash]$ sha256sum CVE-2018-5255-4-20-hotfix.swix
0d74ca3d1ea054d388aece073968c8d2c3d153df861230f2a4bb9871bcb49b58
CVE-2018-5255-4-20-hotfix.swix

[admin@switch flash]$ sha256sum CVE-2018-5255-4-19-hotfix.swix
6ed06ff7b8cc33bfd6b2e50725ff215b0abe1b4d44601d824e31efa0a23cae93
CVE-2018-5255-4-19-hotfix.swix

Note:

- This hotfix can be installed on the affected versions of EOS.
- Installing the patch will restart the MLAG agent that could lead to a momentary disruption in traffic forwarding.
- A reload of the switch is not required for the patch to take effect

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/CVE-2018-5255-4-20-hotfix.swix extens
ion:
switch#verify /sha256 extension:CVE-2018-5255-4-20-hotfix.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 CVE-2018-5255-4-20-hotfix.swix
```

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

```
switch#show extensions
Name                                Version/Release      Status
    Extension
----------------------------------- -------------------- --------
--- ---------
CVE-2018-5255-4-20-hotfix.swix      1.0.2/7318675.\      A, I
    1
                                    vmahadberlinA1\

                                    patch234146.4
```

```
```

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
CVE-2018-5255-4-20-hotfix.swix
```

6. For dual supervisor systems run the above copy command on both active and standby supervisors:

```
switch(s1)#copy installed-extensions boot-extensions
switch(s2-standby)#copy installed-extensions to boot-extensions
```

References:

CVE-2018-5255

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