Date: April 5th, 2018

Version: 1.0

Revision	Date	Changes
1.0	April 5th, 2018	Initial Release

Affected Platforms: All EOS platforms

Affected Software Version: EOS-4.20.1F release.

The CVE-ID tracking this issue is CVE-2018-5254

CVSS v3: 5.0 CVSS:3.0/AV:N/AC:L/PR:L/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 Rib agent may restart if a malicious BGP peer sends an UPDATE message containing a malformed path attribute. Such BGP updates are not expected to be received in typical production environments and have to be crafted and sent with the malformed values by a malicious BGP speaker.

There will be a log message when the switch receives such malformed packets prior to the rib agent restarting.

```
20xx-xx-08T04:27:52.328647+00:00 switch Rib: %BGP-5-UPDATE-ERROR: attribute AS Path i
n update from peer 1.1.1.2 (AS 65502) is malformed, treating as Withdraw.
20xx-xx-08T04:27:52.328647+00:00 switch  Rib: %AGENT-6-INITIALIZED: Agent 'Rib' initi
alized; pid=10873
```

Mitigation:

It is recommended to configure static BGP neighbors with strong BGP authentication keys to protect against unauthorized BGP peers in sending malformed BGP packets.

BUG 229418 tracks this vulnerability. A fix for this issue is available from SW versions 4.20.2F onwards.

Note: This vulnerability was identified internally by Arista Networks and Arista has not received evidence of this being exploited, as of the date of this update.

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:

SecurityAdvisory0033Hotfix.swix

Sha256 sum is:

[admin@switch flash]$ sha256sum SecurityAdvisory0033Hotfix.swix

c0d8bea145222d9e28eca08d429bc3e14f8e30a86495a41501f1fefe84b9713b SecurityAdvisory0033Hotfix.swix

Note:

- This hotfix can be installed on the affected versions of EOS.
- 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/SecurityAdvisory0033Hotfix.swix extension:
switch#verify /sha256 extension:SecurityAdvisory0033Hotfix.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 SecurityAdvisory0033Hotfix.swix
```

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

```
switch#show extensions
Name                                    Version/Release      Status      Extension
--------------------------------------- -------------------- ----------- ---------
SecurityAdvisory0033Hotfix.swix          1.0.0/eng      A, I        1
```

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
SecurityAdvisory0033Hotfix.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-2018-5254

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