Date:December 16th, 2020

Version: 1.0

Revision	Date	Changes
1.0	December 16th, 2020	Initial Release

The CVE-ID tracking this issue is: CVE-2020-24360
CVSSv3.1 Base Score: 7.4/10 (AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H)

Description

This advisory documents the impact of a vulnerability in Arista's EOS affecting the 7800R3, 7500R3 series and the 7280R3 series of products. Affected software releases are listed below. An issue with ARP packets may result in issues that cause a kernel crash, followed by a device reload. Bug 504140 tracks this issue for EOS.

This is an internally found vulnerability and Arista has not received any report of this issue being used in any malicious manner.

Vulnerability Assessment

Affected Software

EOS Versions

- 4.24.2.4F and below releases in the 4.24.x train.
- 4.23.4M and below releases in the 4.23.x train.
- 4.22.6M and below releases in the 4.22.x train

Affected Platforms

This vulnerability affects only the following platforms:

- 7500R3 Series
- 7800R3 Series
- 7280R3 Series

The following products are **not affected:**

- Arista EOS-based products:
    - 7010 series

    - 7020R Series
    - 7050X/X2/X3 series
    - 7060X/X2/X4 series
    - 7150 series
    - 7160 series
    - 7170 series
    - 720XP series
    - 750X series
    - 7250X series
    - 7260X/X3 series
    - 7280E/R/R2 series
    - 7300X/X3 series
    - 7320X series
    - 7368 / X4 series
    - 7500E/R/R2 series
- Arista Wireless Access Points
- CloudVision Wi-Fi, virtual appliance or physical appliance
- CloudVision Wi-Fi cloud service delivery
- CloudVision Portal, virtual appliance or physical appliance
- CloudVision as-a-Service
- Arista 7130 Systems running MOS
- Arista Converged Cloud Fabric and DANZ Monitoring Fabric (Formerly Big Switch Nodes for BCF and BMF)

Symptoms

Platforms from the Arista R3 series running the affected software with both 'ip routing' enabled and Layer 3 interfaces configured, either as a routed port or as an SVI, are vulnerable. The recommendation is to install the hotfix or upgrade to a remediated EOS version. Below are show commands that can help determine if the required configurations are in use. The commands listed below can be used to identify the presence of Layer 3 interfaces and ip routing configuration (relevant outputs highlighted in red). In the example below, Ethernet1 is a routed port and Vlan4000 is an SVI - both are Layer 3 interfaces.

```
switch#show ip interfaces brief


Interface      IP Address         Status       Protocol   MTU
-------------- -----------------  ------------ ----------- ------
Ethernet1      172.
15.100.109/30    up           up       1500
Ethernet2      172.15.100.113/30    up           up       1500

Loopback0      172.15.0.21/32       up           up       65535

Management1    10.90.165.21/24      up           up       1500
```

```
Vlan4000       192.
168.1.2/30       up           up       1500

switch#show run section ip routing
ip routing
```

As a result of the kernel panic, the following (highlighted) function name is displayed in the 'Debugging Information' section in the output of command 'show reload cause':

```
"fab_send_frame_up.constprop.11+0x951/0x193e"
```

Mitigation

If an EOS upgrade to the remediated version is not feasible, a hotfix is available as mitigation against this vulnerability.

The hotfix can be installed as an EOS extension and is applicable across all affected EOS versions. Installing the hotfix is non-disruptive to control plane and data plane traffic.

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

- Patch file download URL: SecurityAdvisory0059Hotfix.swix
- Sha512sum: a33bc69f853269cfac2cf67c57033538100d5c356757ae0381614d10f537a2859db2d40bc29ff0eb37def08f12d15e4288293e25341c2a26453c562c4188730a

Resolution

This vulnerability is tracked by Bug 504140. The recommended resolution is to upgrade to a remediated EOS version.

The vulnerability has been fixed in the following EOS versions:

- 4.25.0F
- 4.24.3M
- 4.23.5M
- 4.22.7M

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