Date: July 2nd, 2019

Version: 1.1

Revision	Date	Changes
1.0	June 26th, 2019	Initial Release
1.1	July 2nd, 2019	Mitigation for CloudVision, MOS, and Wi-Fi products; Updated swix for EOS
1.2	July 24th, 2019	Updated EOS patch for non-default VRFs

The CVE-IDs tracking this issue are CVE-2019-11477, CVE-2019-11478, and CVE-2019-11479.

CVSSv3 Base Score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Description:

The TCP networking vulnerabilities in the Linux kernels relate to Maximum Segment Size (MSS) and TCP Selective Acknowledgement (SACK) capabilities. This series of CVEs around the Linux kernel can be exploited by sending TCP packets to an IP address on the switch. This means the exposure on Arista devices would be on Management ports, Routed ports, SVI interfaces, and other interfaces with IP accessibility.

CVE-2019-11477: SACK Panic (Linux >= 2.6.29). A sequence of specifically crafted SACKs can trigger an integer overflow, possibly leading to a kernel crash. A remote attacker could exploit this to crash the system and create a Denial Of Service.

CVE-2019-11478: SACK Slowness (Linux < 4.15) or Excess Resource Usage (all Linux versions). A sequence of specifically crafted SACKs can cause a fragmented TCP queue, which can possibly lead to slowness or Denial of Service.

CVE-2019-11479: Excess Resource Consumption Due to Low MSS Values (all Linux versions). The low maximum segment size (MSS) can cause an increase of fragmented packets and thereby increase the bandwidth consumption. This vulnerability can create a resource problem in both the CPU and network interface when crafted packets with low MSS values are used, potentially leading to slowness or Denial of Service.

These CVEs were publicly found and the exposure is across the Linux versions as mentioned above. This means that the following Arista products are affected: EOS, MOS, CVP, CVA, and the Wi-Fi products: Wireless Manager, Access Points, and all the Wi-Fi Cloud services. The complete list of affected products and software versions are documented below.

Vulnerability Assessment

Affected Software

The vulnerabilities are in the Linux Kernel, leading to all the currently shipping code versions being impacted.

- EOS
  - 4.22.0F
  - 4.21.6M and below
  - 4.20.13M and below
  - 4.19.12M and below
  - 4.18.11M and below
  - The currently end of support code trains (4.17 and below)
- CloudVision:
  - CVP: 2018.2.4 and below
  - CVA: 2.1.1 and below
- MOS (Metamako OS):
  - 0.21.0 and below
- Wi-Fi
  - Wireless Manager and Access Points: 8.7.1 and below

Affected Platforms

These vulnerabilities are platform independent.

Mitigation

The long-term resolution is upgrade to a remediated code version, as detailed in the next section. A temporary mitigation is to use the hotfix provided for the impacted products.

EOS

The hotfix can be installed as an EOS extension on affected versions (4.17 and later release trains). It is recommended to install a patch on affected versions of EOS to safeguard against this vulnerability.

- [v1.0.0] Patch file download URL: SecurityAdvisory0041Hotfix-EOS-v1.0.0.swix (posted on 06/26); sha512 checksum for verification.
- [v1.0.1] Patch file download URL: SecurityAdvisory0041Hotfix-EOS-v1.0.1.swix (posted on 07/01); sha512sum checksum for verification.
  - v1.0.1 of the hotfix is available to handle a corner case where the iptables rules fail to install with v1.0.0.
  - The mitigation logic is the same for both versions, hence no action is necessary if the rules successfully installed with v1.0.0.
- [v1.0.2] Patch file download URL: SecurityAdvisory0041Hotfix-EOS-v1.0.2.swix (posted

on 07/24); sha512sum checksum for verification.
    - v1.0.2 of the hotfix is available as mitigation when non-default VRFs are in use. No action is needed for users with the initial patch applied, unless coverage for non-default VRF is needed.
    - The mitigation logic is consistent and can be used as a standalone patch

Note:

- The patch installation is platform independent and hitless. A reload of the switch or any process is not required for the patch to take effect.
- The patch has been tested for EOS versions 4.17 and onwards. For releases < 4.17, the recommendation is to upgrade code to a remediated version in any of the supported release trains.
- With the mitigation in place, legitimate packets with TCP Maximum Segment Size (MSS) less than 500 (as announced during the TCP handshake) will be dropped. If such traffic is directly addressed to an IP interface on the device and is expected in the network, the suggestion is to remove the patch and disable TCP SACK to safeguard against the vulnerability.

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-6-7-managing-eos-extensions

- Ensure that the extension is made persistent across reboots by copying the installed-extensions to boot-extensions.

CloudVision Portal

The mitigation for CloudVision Portal can be done by running the following commands in your CVP shell as a root user:

- firewall-cmd --permanent --direct --add-rule ipv4 filter INPUT 0 -p tcp -m tcpmss --mss 1:500 -j DROP
- firewall-cmd --permanent --direct --add-rule ipv6 filter INPUT 0 -p tcp -m tcpmss --mss 1:500 -j DROP
- firewall-cmd --reload

Note:

- These commands need to be executed only once i.e. the mitigation is persistent across reboots.
- This process is hitless to ongoing CVP operations

CloudVision Appliance

The mitigation for CloudVision Appliance can be done by following the below steps after logging in to the CVA shell as a root user:

- Create a daemon file:
    - mkdir /etc/libvirt/hooks && touch /etc/libvirt/hooks/daemon
- Open the daemon file at /etc/libvirt/hooks/daemon using vi or any available editor
- Add the following contents to the daemon file:
  #!/bin/bash
  if ["$2" = "start"]; then
  /sbin/iptables -t filter -I INPUT -p tcp -m tcpmss --mss 1:500 -j DROP
  /sbin/ip6tables -t filter -I INPUT -p tcp -m tcpmss --mss 1:500 -j DROP
  fi
- Exit the editor and make the daemon file executable:
    - sudo chmod a+x /etc/libvirt/hooks/daemon
- Run the following command to execute:
    - /etc/libvirt/hooks/daemon - start - start

Note:

- These commands need to be executed only once i.e. the mitigation is persistent across reboots.
- This process is hitless.

Metamako OS (MOS)

The hotfix can be installed as an application on affected versions (0.21.1 and below). It is recommended to install this patch on affected versions to safeguard against this vulnerability

- Patch file is available on the MOS release page or downloadable directly from this URL: SecurityAdvisory0041Hotfix-MOS.rpm
    - sha512 checksum for verification.

Note:

- Copy the RPM to the device and install as an application
- App install instructions available on EOS Central here and also in Section 5.7 (Application Commands) of the user guide available on the release page.
- Verification of install can be done by checking the syslogs or the applications list in the output of ‘show version’
- The hotfix will remain installed until explicitly removed, though it will not have any effect on the remediated releases. To remove the application, run the command: ‘remove app hotfix-sa41-1.0.0’ at the config prompt

Wi-Fi Products

Wireless Manager (WM) Server

It is recommended to install this patch on affected versions (8.7.1 and below) to safeguard against this vulnerability.

- Patch file download URL: SecurityAdvisory0041Hotfix-WM.tgz
- sha512 checksum for verification

Note:

- The patch should be applied on on-prem WM servers:
  - Login as config user to the WM server and run the command: ‘get debug ondemand’
  - Proactively download the patch locally and provide the path to the patch file when prompted
- Installation is hitless (i.e. reboot or service restart is not required).
- This patch is persistent across reboots and and also independent of server platform, server OS, and server version.
- In CentOS-7 based WM servers using version 8.7.1 and having IPv6 enabled, this mitigation does not persist for IPv6 connections after server reboot.
  - The temporary workaround is to apply the patch again on such servers after reboot. The long-term fix will be available in the WM 8.8 release.

Access Points (APs)

Immediate mitigation is not available for APs. A full build with remediated kernel will be available in the upcoming 8.7.1 hotfix, that is scheduled for GA by mid-July, and the subsequent releases starting 8.8 version.

Wi-Fi Cloud Services

For immediate mitigation, the patch to safeguard against these vulnerabilities has been applied on the Wi-Fi Cloud Services.

Resolution:

The following bugs track this vulnerability and impact across Arista products. The fix requires an update to the kernel and hence the recommended course of action is to upgrade to a fixed code version once it’s available for download. Here are the pertaining Bug IDs and versions with the fix:

EOS

- BUG392663 (CVE-2019-11477)
- BUG392669 (CVE-2019-11478)
- BUG392674 (CVE-2019-11479)
- Fixes will be available in 4.22.1F, 4.21.7M, 4.20.14M , 4.19.13M, 4.18.12M and later releases
- Fix is also available in 4.21.2.3F
- Fix is also available in 4.21.6.1.1F

CloudVision Portal

- BUG393224 (CVE-2019-11477)
- BUG393226 (CVE-2019-11478)
- BUG393227 (CVE-2019-11479)
- Fixes will be available in 2018.2.5, 2019.1.0, and later releases

CloudVision Appliance

- BUG395275 (CVE-2019-11477)
- BUG395279 (CVE-2019-11478)
- BUG395305 (CVE-2019-11479)
- Fixes will be available in 2.1.2 and later releases

MOS

- MOSH-10808 (CVE-2019-11477)
- MOSH-10809 (CVE-2019-11478)
- MOSH-10810 (CVE-2019-11479)
- Fixes will be available in 0.21.1 and later releases

Wi-Fi

Wireless Manager (WM) Server

- BUG393116 (CVE-2019-11477)
- BUG393131 (CVE-2019-11478)
- BUG393133 (CVE-2019-11479)
- Fix to be available in 8.8 and later releases

Access Points (APs)

- BUG393146 (CVE-2019-11477)
- BUG393147 (CVE-2019-11478)
- BUG393148 (CVE-2019-11479)
- Fix to be available in 8.7.1 hotfix, 8.8, and later releases
- The legacy platforms, that are currently End-of-Life, will have the fix available in 8.2.1 version

Wi-Fi Cloud Services

The next upgrade of all Wi-Fi cloud services will have the remediated kernel version. In the meantime, the mitigation to safeguard against these vulnerabilities has already been applied.

Vulnerability References

- https://github.com/Netflix/security-bulletins/blob/master/advisories/third-

party/2019-001.md
- https://nvd.nist.gov/vuln/detail/CVE-2019-11477
- https://nvd.nist.gov/vuln/detail/CVE-2019-11478
- https://nvd.nist.gov/vuln/detail/CVE-2019-11479
- https://access.redhat.com/security/vulnerabilities/tcpsack

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