Date: August 6th, 2018

Version: 1.0

Revision	Date	Changes
1.0	August 6, 2018	Initial Release

Vulnerability assessment of CVE-2018-5390 for Arista Products

CVSS v2: 7.1 (AV:N/AC:M/Au:N/C:N/I:N/A:C)

On August 6th, 2018, information was released about a denial of service vulnerability for TCP connections affecting the Linux kernel, also referred to as SegmentSmack. The vulnerability exploits the worst case algorithmic complexity of TCP stream reassembly in Linux kernels.

Arista EOS, vEOS, and CloudVision Portal are affected products. Affected versions, mitigation, and resolution are documented in the following sections.

Vulnerability Assessment for EOS and vEOS Router:

Affected EOS versions:

All shipping EOS releases as of the date of this advisory are affected. Table below has the complete list of EOS versions:

4.20	4.19	4.18	4.17	4.16	All older release trains
4.20.7M 4.20.6F 4.20.5.2F 4.20.5.1F 4.20.5F 4.20.4.1F 4.20.4F 4.20.3F 4.20.2.1F 4.20.2F 4.20.1F 4.20.0F	4.19.9M 4.19.8M 4.19.7M 4.19.6.3M 4.19.6.2M 4.19.6.1M 4.19.6M 4.19.5M 4.19.4.1M 4.19.4M 4.19.3F 4.19.2.3F 4.19.2.2F 4.19.2.1F 4.19.2F 4.19.1F 4.19.0F	4.18.8M 4.18.7M 4.18.6M 4.18.5M 4.18.4.2F 4.18.4.1F 4.18.4F 4.18.3.1F 4.18.3F 4.18.2.1F 4.18.2F 4.18.1.1F 4.18.1F 4.18.0F	4.17.9M 4.17.8M 4.17.7M 4.17.6M 4.17.5.1M 4.17.5M 4.17.4M 4.17.3F 4.17.2.1F 4.17.2F 4.17.1.4F 4.17.1.1F 4.17.1F 4.17.0F	4.16.14M 4.16.13M 4.16.12M 4.16.11M 4.16.10M 4.16.9M 4.16.8M 4.16.7M 4.16.6M	All releases in 4.15 All release trains older than 4.15

Affected Platforms

This vulnerability is in the Linux kernel and hence affects all platforms running EOS in the Arista product family.

Affected vEOS Router versions:

EOS-4.20.6FX-Virtual-Router
EOS-4.20.5F
EOS-4.20.1FX-Virtual-Router
EOS-4.18.0FX-VEOS

Symptoms

Symptoms of the exploit are similar to that of packet starvation at the CPU. Latency sensitive protocols such as BFD, may timeout based on the configured timers.
The following symptoms may show up in EOS because of this vulnerability

1. High CPU usage on CPU1 (additionally CPU2 on some modular systems)
2. Latency sensitive protocols such as BFD, STP and LACP may flap as processing of their packets is delayed
3. Reduced packet processing capacity may affect sflow sampling
4. Reduced packet processing capacity may delay events, such as BGP convergence or copying files, where many packets are exchanged

Mitigation

1. The TCP segment vulnerability can be mitigated across all platforms by configuring ACLs to drop/deny packets to the control plane from untrusted hosts.
As security best practice, it is always recommended to block untrusted hosts from accessing open ports on the control plane using control plane ACLs. It is also recommended to monitor for high CPU usage (~100% of a single core) to get visibility into trusted hosts being compromised or spoofed.
Below is a sample ACL that can be applied to the control plane to deny untrusted hosts.

1. The first step is to determine which hosts or peers are expected to communicate with the switch. In this example we'll allow the specific host 10.5.4.3 and any host from the subnet 192.168.10.0/24.
2. Once this has been determined an IP access list which permits these hosts and denies all other traffic should be created:

```
(config)# ip access-list cve
(config-acl-cve)# permit ip host 10.5.4.3 any
(config-acl-cve)# permit ip 192.168.10.0/24 any
(config-acl-cve)# exit
(config)# show ip access-lists cve
IP Access List cve
        10 permit ip host 10.5.4.3 any
```

```
        20 permit ip 192.168.10.0/24 any
```

3. This access list must then be applied to the control plane to provide protection. This can be done either using control plane ACLs or Service ACLs based on EOS version (Refer to table below). Where supported control-plane ACLs are preferred.
   To apply a control-plane ACL:

```
(config)# control-plane
(config-cp)# ip access-group cve in
```

   Service ACLs must be applied to each service.. As an example, a Service ACL can be applied to the SSH service as shown below. See the Service ACLs section of the EOS configuration guide for the complete list of services:

```
(config)# management ssh
(config-mgmt-ssh)# ip access-group cve in
```

NOTE: Control plane ACLs are are not supported in any the following EOS releases*:

- 4.19.0 - 4.19.8M
- 4.20.0F - 4.20.4F
- 4.20.5F - 4.20.6F

The mitigation using service ACLs is recommended for EOS versions that do not support control plane ACLs.
* The above restriction does not apply to EOS-INT (International) images for the specified releases.

2. In order to monitor for high CPU usage, the EOS CLI command “show proc top” can be used. Run the command and then press “1” to enable the per-CPU summary view. The lines to monitor for high usage are “si” under %CPU1 and %CPU2 as these denote the percentage of time spent on kernel processes such as packet processing:

```
top - 09:29:57 up 11 min, 2 users,  load average: 0.38, 0.65, 0.54
Tasks: 288 total,   1 running, 287 sleeping, 0 stopped,   0 zombie
%Cpu0:1.7 us, 0.7 sy, 0.0 ni, 97.4 id, 0.0 wa,0.3 hi,0.0 si,0.0 st
%Cpu1:6.0 us, 0.3 sy, 0.0 ni, 93.4 id, 0.0 wa,0.3 hi,0.0 si,0.0 st
%Cpu2:3.3 us, 0.7 sy, 0.0 ni, 95.7 id, 0.0 wa,0.3 hi,0.0 si,0.0 st
%Cpu3:3.7 us, 0.7 sy, 0.0 ni, 95.7 id, 0.0 wa,0.0 hi,0.0 si,0.0 st
KiB Mem:3817912 total, 1705348 used, 2112564 free, 9256 buffers
KiB Swap:0 total,        0 used,        0 free,   811276 cached
```

Values of “si” for either %CPU1 or %CPU2 greater than 90.0% indicate a strong possibility the system is being attacked.

Resolution:

Bug 278852 tracks this vulnerability for EOS and vEOS. The fix for CVE-2018-5390 will be available in the following versions:
EOS-4.21.2.3F, EOS-4.21.0F, EOS-4.20.8M, EOS-4.19.10M, EOS-4.18.9M, EOS-4.17.10M

Please leverage the mitigation steps explained in this advisory until the fixed-in versions are deployed.

Vulnerability assessment for CloudVision Portal

Affected CloudVision Portal versions:

2018	2017	2016	2015
2018.1 • 2018.1.2.1 • 2018.1.2 • 2018.1.1 • 2018.1.0	2017.2 • 2017.2.3 • 2017.2.2 • 2017.2.1 • 2017.2.0 2017.1 • 2017.1.1.1 • 2017.1.1 • 2017.1.0.1 • 2017.1.0	2016.1 • 2016.1.2.3 • 2016.1.2.1 • 2016.1.2 • 2016.1.1 • 2016.1.0	2015.1 • 2015.1.2 • 2015.1.1
All shipping versions of CloudVision Appliance running 2.0.0 and below are affected			

Symptoms

Symptoms of the exploit are similar to that of packet starvation at the CPU. The following symptoms may show up on the operating system hosting CloudVision Portal because of this vulnerability:

1. High CPU usage on one core
2. Reduced packet processing capacity
3. Reduced packet processing capacity may result in delayed response from the CVP user interface

Mitigation:

Follow best practices to ensure that the application or host is not accessible over the internet and access is restricted to a trusted set of IP addresses or a subnet. Monitor CPU usage for symptoms specified above. Recommendation is to upgrade to the remediated version of CVP.

To identify the version of the CVA release on the CloudVision Appliance, run the following command on an SSH session to the CloudVision Appliance:

- cat /etc/cva-version.txt (On systems running versions earlier than CVA-2.0.0)
- cat /cva/version.txt (For systems running 2.0.0 and later releases)

Resolution:

Bug 279911 tracks this issue for CloudVision Portal. The fix will be available in the following version of CloudVision Portal:

- CloudVisionPortal-2018.2.0

Vulnerability References:

More information on CVE-2018-5390 can be found here:

https://www.kb.cert.org/vuls/id/962459

https://nvd.nist.gov/vuln/detail/CVE-2018-5390

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