Date: August 14th, 2018

Last Updated: March 25th, 2019

Version: 1.1

Revision	Date	Changes
1.0	August 14, 2018	Initial Release
1.1	March 25, 2019	Updated with Remediated versions

The CVE-ID tracking this issue is CVE-2018-5391

CVSS v2: 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

Description

On August 14th, 2018, information was released about a denial of service vulnerability where a crafted IP fragment ordering or overlap can allow an attacker to consume much more memory than defined in the Linux kernel settings.

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

Vulnerability Assessment for EOS and vEOS Router:

Affected EOS versions:

EOS releases with Linux kernel version 3.18 are susceptible to this vulnerability. Affected releases are listed below. The release trains prior to EOS-4.20 run version 3.4 of the Linux kernel which is not vulnerable to this CVE.

4.20	4.21
4.20.8M 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	4.21.0F

4.20.0F	

Affected Platforms

This vulnerability is in the Linux kernel and hence affects all platforms running the affected EOS releases.

Affected vEOS Router versions:

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

Symptoms

Symptoms of the exploit are similar to that of high memory consumption on a device. As a result of the increased memory consumption, the system exhibits symptoms that may include alerts for high memory utilization on monitoring tools, an Out Of Memory (OOM) condition on the system resulting in EOS agents restarts as they are unable to reserve sufficient memory.

The following symptoms are a result of high memory usage in EOS:

- High memory usage (show proc top memory)
- Restart of agents consuming high memory (show logging system)
- OOM condition for agents unable to reserve memory for functioning (show logging all)
- Packet forwarding issues and/or network protocols being impacted, depending on the memory lock-up and memory requirement of the device

Typically, a system running EOS is not expected to receive a large number of IP fragments. As a result a major symptom would be any system receiving lots of fragments (unless TCP/UDP MTU discovery is disabled or broken somewhere in the network).

The number of IP fragments received by the kernel can be retrieved, per VRF, using the command: *show kernel ip counters| grep 'reassemblies required'*

Mitigation

It is recommended to install this patch on affected versions of EOS/vEOS to safeguard against this vulnerability.

Patch file download URL: SecurityAdvisory0037Hotfix.swix

sha256 sum is:
f3e2c489bcb78f5a5f0afc79ffd8e851064083d6aeaf8b82b24ecfec7d0d15e6
sha512sum is:
5a629438fd9988bb2ad8ece630355a033997200febf723ab531825f33b355c647b14957983fda91a131c6dc1d31f78fc0bee8fb092e6d17d6c9036921f7e6849

Note:

- This hotfix is version agnostic (i.e. can be installed on any affected version)
- The patch installation is hitless and 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/SecurityAdvisory0037Hotfix.swix
extension:
switch#verify /sha256 extension:SecurityAdvisory0037Hotfix.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 SecurityAdvisory0037Hotfix.swix
```

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

```
switch#show extensions
Name                    Version/Release      Status      Extension
----------------------- -------------------- ----------- ---------
SecurityAdvisory0037Hotfix.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
SecurityAdvisory0037Hotfix.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 boot-extensions
```

Additionally, it is always recommended to follow security best practices to protect the control plane by using access lists to restrict access to trusted hosts.

Resolution:

Bug 280955 tracks this vulnerability for EOS and vEOS. The fix for CVE-2018-5391 is available EOS versions 4.21.2.3F, 4.20.9M, 4.21.1F and later releases.

Please install the provided hotfix as a mitigation until the remediated versions are available.

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 are affected (1.0.0, 1.2.0, 2.0.0)			

Symptoms

Symptoms of the exploit are similar to that of high memory consumption. Alerts for low available memory and process restarts may be observed as a result of OOM (Out of Memory) condition. This may also manifest as sluggish or slow response from the user interface while using CloudVision Portal.

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 memory usage of the Operating System hosting the CloudVision Portal. Recommendation is to upgrade to the remediated version of CVP.

Resolution:

Bug 282178 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-2018-5391 can be found here:

https://www.kb.cert.org/vuls/id/641765

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