Date: October 31st, 2017

Version: 1.6

Revision	Date	Changes
1.0	February 16th, 2016	Initial release
1.1	February 19th, 2016	Updates include assessment and mitigation
1.2	February 25th, 2016	Updates include options for mitigation and protection on affected EOS releases
1.3	April 6th, 2016	Updates include patch install instructions for modular systems
1.4	April 8th, 2016	Updates include availability of releases with the glibc fix
1.5	June 5th, 2017	Updated to include new version of patch file for EOS to address a bug in the original version - SecurityAdvisory0017-nonDisruptive-v1.1.swix
1.6	October 31st, 2017	Updated to include new version of patch file to address an issue with the previous version. The updated version is SecurityAdvisory0017-nonDisruptive-v1.2.swix

Arista Products vulnerability report for security vulnerabilities released for glibc getaddrinfo() in February, 2016

Google and Redhat have released information on a stack based buffer overflow for the glibc function getaddrinfo(). glibc is a C library used in the GNU system and in GNU/Linux systems, as well as many other systems that use Linux as the kernel. This advisory has been updated to reflect the vulnerability status for Arista products. Arista EOS and CloudVision are vulnerable to CVE-2015-7547.

CVE-2015-7547: (glibc getaddrinfo stack-based buffer overflow)

Table-1: Arista Products vulnerability assessment

Product:	EOS
Software versions:	All EOS releases shipped prior to the date of this release are affected. The list of affected releases is documented in Table-2
Status:	Vulnerable
Details	Mitigation and resolution are documented in the following sections of this advisory. Bug ID 147810 tracks this vulnerability for EOS. A software fix will be available for the currently active EOS software trains, in particular EOS versions 4.15.5M, 4.14.12M and 4.13.15M.
Product:	CloudVision
Software versions:	CloudVision Portal 2015.1, 2015.1.1, 2015.1.2
Status:	Vulnerable
Details	Patch instructions are documented in the following sections of this advisory. Bug ID 148109 tracks this vulnerability for CloudVision Portal. The fix will be available in CVP version 2016.1.

Product: EOS

Table-2: EOS releases with affected version of glibc

4.15	4.14	4.13	4.12	Older release trains
4.15.0F • 4.15.0FX • 4.15.0FXA • 4.15.0FX1 4.15.1F	4.14.0F 4.14.1F 4.14.2F 4.14.3F 4.14.3.1F 4.14.4F 4.14.4.1F 4.14.4.2F 4.14.5F	4.13.1.1F 4.13.2.1F 4.13.3.1F 4.13.4.1F 4.13.5F 4.13.5.1F 4.13.6F 4.13.7M 4.13.7.2M 4.13.7.3M	4.12.5.2 4.12.6.1 4.12.7.1 4.12.8 4.12.8.1 4.12.9 4.12.10 4.12.11	All releases in 4.11 All releases in 4.10 All releases in 4.9 All releases in 4.8 All releases in 4.7

• 4.15.1FX B1 • 4.15.1FX B • 4.15.1FX -7060X • 4.15.1FX -7260QX 4.15.2F 4.15.3F • 4.15.3FX -7050X-72Q • 4.15.3FX -7060X.1 • 4.15.3FX -7500E3 • 4.15.3FX -7500E3.3 4.15.4F • 4.15.4FX -7500E3	• 4.14.5FX • 4.14.5FX .1 • 4.14.5FX .2 • 4.14.5FX .3 • 4.14.5FX .4 • 4.14.5.1F-SSU 4.14.6M 4.14.7M 4.14.7.1M 4.14.8M 4.14.8.1M 4.14.9M 4.14.10M 4.14.11M	4.13.8M 4.13.9M 4.13.9.1M 4.13.10M 4.13.11M 4.13.12M 4.13.13M 4.13.14M		All releases in 4.6 All releases in 4.5 All release trains older than 4.5

Recommended Next Steps for affected EOS releases

The following options are available or in progress as actions to mitigate or protect against this vulnerability:

Option 1. Mitigation against known attack vector using an extension. The installation of this extension is non-disruptive to switch operation. **(Status: Available)**

Option 2. Patched glibc libraries. This option provides complete protection against the vulnerability. However, a reboot of the switch is required for the patched libraries to take effect. **(Status: Available)**

Option 3. EOS releases with remediated versions of glibc. EOS versions 4.15.5M, 4.14.12M and 4.13.15M include the fix. **(Status: Available)**

Option 1: Mitigation against known attack vector using an extension

While Arista EOS is vulnerable, the Proof of Concept code published as part of the vulnerability disclosure is not directly effective as a test against affected EOS versions. There have been no external reports of an exploit against EOS as of the date of this notice. As noted in Google's report of the vulnerability, the attack vectors for this vulnerability are diverse. The following procedure provides mitigation only against the known attack vector that exploits the vulnerability in the glibc DNS client side resolver. The mitigation involves installing an extension that installs rules in IPtables in Linux to drop UDP responses from non-compliant or hostile DNS servers. The extension also sets up dnsmasq to switch to TCP for DNS responses larger than 1024 bytes from compliant DNS servers. The IPtables rules is installed for IPv4, IPv6 and applies to name-servers configured in both the default and customer defined VRFs.

NOTE:

- If SecurityAdvisory0017-nonDisruptive-v1.1.swix is installed while the original SecurityAdvisory0017-nonDisruptive.swix is still installed, it might lead to some duplicate entries in dnsmasq.conf file. As a workaround uninstall v1.1 and v1.0 and then install SecurityAdvisory0017-nonDisruptive-v1.1.swix.
  This issue is fixed in an updated SecurityAdvisory0017-nonDisruptive-v1.2.swix patch.
- The extension can be installed even if the IPtables rules have already been applied
- The extension can be installed on all affected EOS versions
- Installing this extension is non-disruptive to the switch operation
- The extension re-installs the IPtables rules every time a change is made to the control plane ACL at which time there is a gap of at most one minute before the rules are installed

Download URL: SecurityAdvisory0017-nonDisruptive-v1.2.swix

sha512sum:

```
7de2a2395d4e04565a82db3dd25386f59d24964d3d4bb0e8921f4cd4ccf9114692e38335b6433b68afe22
34f33c3253f2291e8221c454d2341ef4ee4cc88ca15
```

NOTE (Updated June 5th, 2017): Document revision 1.5 includes an updated version of the above listed non-disruptive patch (v1.1) to address an issue that was identified with the original version of the patch. On a long running switch with the patch installed, every update to IPtables would generate an email filling up the filesystem resulting in an out of memory condition that could potentially cause a kernel panic and reload the switch. It is recommended to install v1.1 of the patch or upgrade to the remediated release. To uninstall the older version of the patch, please follow the rollback instructions documented below. The install instructions can be used to install the updated version of the patch.

Install Instructions

1. Copy the extension using one of the supported file transfer protocols to the extension partition of the switch:

```
switch#copy
scp://user@10.1.1.1//SecurityAdvisory0017-nonDisruptive-v1.2.swix
extension:
```

Verify the integrity of the file by comparing the sha512 with the one provided above:

```
switch#verify /sha512
extension:SecurityAdvisory0017-nonDisruptive-v1.2.swix
```

On modular switches, copy the file to the flash of the peer supervisor using the following commands:

```
switch(s1)#copy extension:SecurityAdvisory0017-nonDisruptive-v1.2.swix
supervisor-peer:mnt/flash/
Copy completed successfully.
switch(s2-standby)#copy
flash:SecurityAdvisory0017-nonDisruptive-v1.2.swix  extension:
```

2. Install the extension using the extension command:

```
switch#extension SecurityAdvisory0017-nonDisruptive-v1.2.swix
```

On modular systems with dual supervisors, the patch has to be installed on the active and standby supervisors:

```
switch(s1)#extension SecurityAdvisory0017-nonDisruptive-v1.2.swix
switch(s2-standby)#extension SecurityAdvisory0017-nonDisruptive-v1.2.swix
```

The extension updates the SuperServer agent. As a result the SuperServer agent will be restarted and this does not impact switch operation. The following message will be logged for the agent restart (PIDs may vary):

```
ProcMgr-worker: %PROCMGR-6-PROCESS_TERMINATED: 'SuperServer' (PID=2026) has te
rminated.
ProcMgr-worker: %PROCMGR-6-PROCESS_RESTART: Restarting 'SuperServer' immediate
ly (it had PID=2026)
ProcMgr-worker: %PROCMGR-6-PROCESS_STARTED: 'SuperServer' starting with PID=19
317 (PPID=1736) -- execing '/usr/bin/SuperServer'
```

3. The following command can be used to verify that the extension is installed:

```
switch#show extensions
```

```
Name                                              Version/Release      Status
   Extension
------------------------------------------------- ------------------- ---------
-- ---------
SecurityAdvisory0017-nonDisruptive-
v1.2.s\      2.6.0/5426905.\      A, I        1
wix                                               gamiltonsecAdv\

                                                  isory0017Patch\

                                                  .11

A: available | NA: not available | I: installed | NI: not installed | F: force
d
```

4. The following command and outputs can be used to verify that the IPtables rules have been installed:

```
switch#bash sudo iptables -L | grep domain
DROP    udp  --  anywhere    anywhere  udp spt:domain length 1500:65535
```

For name servers configured in VRFs, the following command can be used:

```
switch#bash sudo ip netns exec ns-<VRF-name> iptables -L | grep domain
```

5. Run the following command to make the extension persist across reloads:

```
switch#copy installed-extensions boot-extensions
switch#show boot-extensions
SecurityAdvisory0017-nonDisruptive-v1.2.swix
```

For dual supervisor systems run the copy command on both active and standby supervisors:

```
switch(s1)#copy installed-extensions boot-extensions
switch(s2-standby)#copy installed-extensions to boot-extensions
```

Rollback Instructions: Uninstalling the extension will remove the IPtables rules and the DNS packet size negotiation and will restart the SuperServer agent.

1. Uninstall the extension using the following command:

```
switch#no extension SecurityAdvisory0017-nonDisruptive-v1.2.swix
```

On modular systems with dual supervisors, the patch has to be uninstalled on the active and standby supervisors:

```
switch(s1)#no extension SecurityAdvisory0017-nonDisruptive-v1.2.swix
switch(s2-standby)#no extension SecurityAdvisory0017-nonDisruptive-v1.2.swix

switch#show extensions
Name                                            Version/Release      Status
   Extension
------------------------------------------------ -------------------- ---------
-- ---------
SecurityAdvisory0017-nonDisruptive-
v1.2.s\      2.6.0/5426905.\      A, I        1
wix                                             gamiltonsecAdv\

                                                isory0017Patch\

                                                .11

A: available | NA: not available | I: installed | NI: not installed | F: force
d
```

2. The SuperServer agent will be restarted as a result of removing the extension and the following messages will be logged (PIDs will vary):

```
%PROCMGR-6-PROCESS_TERMINATED: 'SuperServer' (PID=19317) has terminated.
%PROCMGR-6-PROCESS_RESTART: Restarting 'SuperServer' immediately (it had PID=1
9317)
%PROCMGR-6-PROCESS_STARTED: 'SuperServer' starting with PID=21471 (PPID=1736)
-- execing '/usr/bin/SuperServer'
```

3. Save the changes to boot-extension:

```
switch#copy installed-extensions boot-extensions
switch#show boot-extensions
```

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
```

Upgrade Considerations:

- Since the extension is only a mitigation against a known attack vector, it is recommended to uninstall the extension by following the above procedure before upgrading to a remediated EOS version that offers complete protection against the vulnerability

Option 2: Patched glibc libraries

An extension is available that packages the patched glibc libraries. A reload of the switch is required post installation for the patched libraries to take effect. While disruptive, this method offers complete protection against all attack vectors for this vulnerability. This extension can be installed on all affected EOS releases.

Download URL: SecurityAdvisory0017-glibc.swix

sha512sum:

```
ccdf8ad84ac1a7985d89b026a6a311533a0f028c4a80c9a8fafa9b1ac4386fe169adb15145faea2e8c8f8
cc8e9152f42150c9bd7df63b4dbd4612641d9aabded
```

Install Instructions:

1. Copy the extension using one of the supported file transfer protocols to the extension partition of the switch:

   ```
   switch#copy scp://user@10.1.1.1//SecurityAdvisory0017-glibc.swix extension:
   ```

   Verify the integrity of the file by comparing the sha512 with the one provided above:

   ```
   switch#verify /sha512 extension:SecurityAdvisory0017-glibc.swix
   ```

   On modular systems with dual supervisors, download the file to the extension partition of the active supervisor and copy it to the standby supervisor using the following two commands:

   ```
   switch(s1)(config)#copy extension:SecurityAdvisory0017-glibc.swix
   supervisor-peer:/mnt/flash
   switch(s2-standby)#copy flash:SecurityAdvisory0017-glibc.swix
    extension:
   ```

2. Install the extension using the extension command:

   ```
   switch#extension SecurityAdvisory0017-glibc.swix
   ```

   On modular systems with dual supervisors, the patch has to be installed on the active

and standby supervisors:

```
switch(s1)#extension SecurityAdvisory0017-glibc.swix
switch(s2-standby)#extension SecurityAdvisory0017-glibc.swix
```

3. Save the extension to boot-extensions:

```
switch#copy installed-extensions boot-extensions
switch#show boot-extensions
SecurityAdvisory0017-glibc.swix
```

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
```

4. Reload the switch. On dual supervisor systems reload the standby supervisor first to enable switchover. Once supervisor switchover is successful, reload the current standby.
   NOTE: Supervisor redundancy modes are can be viewed using the command ‘show redundancy states’. It is important to understand the level of redundancy provided by each mode and platform support before initiating a supervisor switchover. Refer to the Supervisor Redundancy chapter of the EOS Configuration Guide for further details.
5. Once the switch is accessible, verify that the new libraries are installed using the following command and the release and version match the following output:

```
switch#bash rpm -qi glibc
Name        : glibc                 Relocations: (not relocatable)
Version     : 2.13                       Vendor: (none)
Release     : 4Ar                     Build Date: Tue Feb 23 14:23:47 2016
```

Rollback Instructions: A reload of the switch is required to rollback to the original version of glibc. The extension cannot be uninstalled using ‘no extension’ due to the dependencies of user processes on glibc. Prior to a reload, remove the extension from boot-extensions by editing the file boot-extensions in the ‘vi’ editor. This requires the user to have access to the bash shell:

```
switch#bash
Arista Networks EOS shell
[admin@switch ~]$ vi /mnt/flash/boot-extensions
```

Use the editor remove the line with the file name SecurityAdvisory0017-glibc.swix and save the changes.

- Navigate the cursor to the line with the extension file name and use ‘dd’ to delete the line
- Enter the following sequence to save the file and quit the editor ‘:wq’

Verify that the extension is no longer present by running ‘show boot-extensions’. For systems with dual supervisors, the boot-extensions file should be edited on both supervisor modules. Reload the switch. On dual supervisor systems reload the standby supervisor first to enable switchover. Once supervisor switchover is successful, reload the current standby

Upgrade Considerations:

- When upgrading to a remediated version of EOS, please follow the rollback instructions to remove the file from boot-extensions before the upgrade

---

Product: CloudVision Portal

Patch installation instructions for CloudVision Portal:

Download URL: CVP-CVE-2015-7547.tgz

```
sha512sum: ed335c89e7b90158b4b21a57d3ccf2f6c3ce1b9810fa48c55ab528afc88101646890cc01b96a1e8c421a7f4e22691d0035e71bf6ba0348244b7c25a9dc34c86c
```

NOTE:

- The patch should be run as ‘root’ user
- This patch is disruptive since it will require a reboot to take effect.

1. Login onto the CVP console as ‘root’ and your root password. This will drop you into a Bash shell.
2. Download the compressed tar file from the URL provided above and copy it to /root Verify sha512 checksum and ensure it is same as the one listed at the top of this document.

   ```
   # sha512sum CVP-CVE-2015-7547.tgz
   ```
3. Untar and uncompress using following command:

   ```
   #tar -zxvf CVP-CVE-2015-7547.tgz
   ```

This will create a directory called ‘cvpupdate’ under your current working directory /root/.

4. Change directory to cvpupdate

```
#cd cvpupdate
```

5. Now execute install.sh

```
#./install.sh
```

6. Running the script will install the patched RPMs for glibc - glibc-2.17-106.el7_2.4.x86_64.rpm & glibc-common-2.17-106.el7_2.4.x86_64.rpm
7. Presence of these rpms can be checked via the following command. The number to note is ‘2.4’ as highlighted below.

```
#rpm -qa | grep glibc
glibc-2.17-106.el7_2.4.x86_64
glibc-common-2.17-106.el7_2.4.x86_64
```

8. This completes the installation process. For the new code to take effect, we need to reboot the CVP VM. Please note that this is disruptive.

```
#reboot
```

After a reboot, the Proof of Concept code provided in the announcement of the vulnerability will serve as a test to confirm that the patch is successful in protecting against the vulnerability.

Multinode considerations:

- This procedure has to be repeated for each and every member of a CVP cluster in a staggered fashion.

Rollback instructions for patch

- To uninstall the patch, login as root and run

```
#yum downgrade glibc glibc-common
```

- Reboot using ‘reboot’

References:

For more information on these vulnerabilities please visit:

CVE-2015-7547: glibc getaddrinfo stack-based buffer overflow

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