Date: 6/9/2014

Revision	Date	Changes
1.0	June 9th 2014	Initial release
1.1	June 12th 2014	Addition of patch installation details
1.2	July 6th 2015	Updated patch file

Open SSL clients running on Arista EOS vulnerable to SSL/TLS MITM vulnerability (CVE-2014-0224)

On June 5th, the OpenSSL project issued a security advisory for a vulnerability that could allow a man in the middle attack (MITM) against an encrypted connection. The attack can only be performed between a vulnerable client *and* server. OpenSSL clients are vulnerable in all versions of OpenSSL. Servers are only known to be vulnerable in OpenSSL 1.0.1 and 1.0.2-beta1.

All current shipping versions of EOS are affected by this vulnerability. Features that use SSL clients and are therefore impacted are XMPP and the "copy" command from the CLI when used in a manner that would involve SSL (i.e. by using a https:// URL). Features in EOS not impacted that run SSL Servers are CAPI, VMTracer and WBEM. These features are not impacted because EOS uses Openssl-1.0.0e which is not a vulnerable version.

A software patch (RPM extension) is available for download. In addition currently supported versions of EOS will receive an updated version with the fix for this vulnerability. Currently supported versions of EOS include 4.9 through 4.13.

BugID 90769 addresses this issue.

Workaround:
To mitigate this issue customers can:

1. Use SCP as an alternative to “https copy” commands.
2. Ensure servers are running remediated versions of OpenSSL or alternate SSL solutions.

References:
For more information about the vulnerability, please visit:
http://www.openssl.org/news/secadv_20140605.txt

Verification:
Verification of the OpenSSL version running in EOS

```
switch# show version detail |grep -i openssl
openssl 1.0.0e.Ar 1709429.4134F.1
```

Resolution:
The resolution to this issue is through the installation of a patch, or through upgrading to a version of EOS that contains the resolution. This section will be updated once EOS releases are available.

Download URL for patch: SecurityAdvisory0005Patch.swix

??Instructions to install the patch for Security Advisory 0005

The extension is applicable for all EOS versions 4.9.0 - 4.13.6 inclusive.

Step 1. Copy the file SecurityAdvisory0005Patch.swix to the extension partition of the Arista switch using any of the supported file transfer protocols:

```
switch#copy scp://arista@10.10.10.123/home/arista/SecAdvisory005Patch.swix extension:
```

Step 2. Ensure that the file has been copied to the extensions partition and verify the checksum of the copied file:

```
switch#show extensions
Name Version/Release Status RPMs
------------------------------------ ------------------------ ------ ----
SecurityAdvisory0005Patch.swix 1.0.0e.Ar/2506963.secAdvi A, NI 1

A: available | NA: not available | I: installed | NI: not installed | F:forced
```

```
sha512sum: f7bdda045eb15d72cdb2c7bce709d7ebfef4b796667b41becd441c87511a093388d9eb5fab
240c97a6addddc4d1a02a430fb1c8cb88e4a9385408e6cb13cb0bf
```

```
switch#verify /sha512 extension:SecurityAdvisory0005Patch.swix
verify /sha512 (extension:SecurityAdvisory0005Patch.2.swix) = f7bdda045eb15d72cdb2c7b
ce709d7ebfef4b796667b41becd441c87511a093388d9eb5fab240c97a6addddc4d1a02a430fb1c8cb88e
4a9385408e6cb13cb0bf
```

Step 3. The patch is installed as an extension, and upon installation into a live system will automatically install with the following behavior:

- Cause ProcMgr to reload it's cached dynamic libraries, including the libssl library containing the change (Impact: Non-disruptive)
- Restart the FastClid-server (Impact: Non-disruptive)
- Restart the Xmpp agent if it is running (Impact: Brief disruption to the Xmpp service only)

```
switch#extension SecurityAdvisory0005Patch.swix
```

Notes:

1. All modular switches with dual supervisors require the extension copying and installing on both supervisors.
2. For systems that have not been patched it is possible when installing the extension it may claim a newer version is already installed. It is recommended to install the extension with the “force” keyword at that point.

Once installed, a series of log messages are expected as shown below.
ProcMgr warm restart to reload cached dynamic libraries:

```
Jun 12 12:27:54 sq393 ProcMgr-
master: %PROCMGR-6-MASTER_STARTED: Master ProcMgr process started. (PID=24770)
Jun 12 12:27:54 sq393 ProcMgr-master: %PROCMGR-6-MASTER_RUNNING: Master ProcMgr (PID=
24770) monitoring ProcMgr worker (PID=24771)
Jun 12 12:27:54 sq393 ProcMgr-worker: %PROCMGR-6-WORKER_COLDSTART: New ProcMgr worker
 cold start. (PID=24771) (Master ProcMgr PID=24770)
Jun 12 12:27:54 sq393 ProcMgr-
worker: %PROCMGR-6-WORKER_WARMSTART: ProcMgr worker warm start. (PID=24771)
Jun 12 12:27:54 sq393 ProcMgr-worker: %PROCMGR-7-NEW_PROCESSES: New processes configu
red to run under ProcMgr control: ['Aaa', 'Acl', 'AgentMonitor', 'Arp', 'Bfd', 'CpuCo
mplex', 'DhcpRelay', 'Dot1x', 'Ebra', 'EventMon', 'FanDetector', 'FastClid', 'Fhrp',
 'Fru', 'IgmpHostProxy', 'IgmpSnooping', 'Ira', 'LacpTxAgent', 'Lag', 'Launcher', 'Led
Policy', 'Lldp', 'Lm73', 'Max6658', 'Mirroring', 'Mlag', 'MlagTunnel', 'Mpls', 'Msdp'
, 'NetworkTopology', 'PciBus', 'PhyEthtool', 'Picasso', 'Pmbus', 'PortSec', 'PowerMan
ager', 'PowerSupplyDetector', 'Qos', 'Rib', 'Sb820', 'Scd', 'Smbus', 'Snmp', 'Sol', '
Stp', 'StpTopology', 'Strata-FixedSystem', 'StrataCentral', 'SuperServer', 'Sysdb', '
Thermostat', 'TopoAgent', 'Ucd9012', 'Xcvr']
Jun 12 12:27:54 sq393 ProcMgr-worker: %PROCMGR-7-PROCESSES_ADOPTED: ProcMgr (PID=2477
1) adopted running processes: (Stp, PID=2560) (SuperServer, PID=1922) (Sysdb, PID=166
8) (Bfd, PID=2053) (Fru, PID=1670) (Launcher, PID=1671) (Qos, PID=2056) (Smbus, PID=2
826) (LedPolicy, PID=2190) (FanDetector, PID=2937) (Rib, PID=2193) (Xcvr, PID=2966) (
LacpTxAgent, PID=1945) (AgentMonitor, PID=1946) (Mirroring, PID=1947) (Ebra, PID=2103
) (Mlag, PID=2011) (NetworkTopology, PID=1972) (PhyEthtool, PID=2889) (Ira, PID=2055)
 (PowerManager, PID=2099) (EventMon, PID=2484) (Fhrp, PID=2101) (Lag, PID=2486) (Igmp
Snooping, PID=1975) (Pmbus, PID=3079) (Aaa, PID=2361) (DhcpRelay, PID=2364) (Arp, PID
=2295) (StrataCentral, PID=3010) (Acl, PID=1974) (Snmp, PID=2249) (Mpls, PID=2378) (S
```

```
ol, PID=2679) (Lm73, PID=2914) (IgmpHostProxy, PID=2126) (Ucd9012, PID=2771) (Sb820,
PID=2773) (PciBus, PID=2775) (StpTopology, PID=2523) (Max6658, PID=2910) (CpuComplex,
 PID=2911) (PowerSupplyDetector, PID=2913) (PortSec, PID=2146) (MlagTunnel, PID=2228)
 (Strata-FixedSystem, PID=3177) (Picasso, PID=2410) (Msdp, PID=2414) (TopoAgent, PID=
2035) (Dot1x, PID=2036) (Scd, PID=2807) (Lldp, PID=2553) (Thermostat, PID=2298)
Jun 12 12:27:54 sq393 ProcMgr-worker: %PROCMGR-7-WORKER_WARMSTART_DONE: ProcMgr worke
r warm start done. (PID=24771)
```

Restart of FastClid process:

```
Jun 12 12:27:54 sq393 ProcMgr-worker: %PROCMGR-6-PROCESS_STARTED: 'FastClid' starting
 with PID=24772 (PPID=24771) -- execing '/usr/bin/FastClid'
```

Restart of Xmpp process:

```
Jun 12 16:09:16 sq393 ProcMgr-worker: %PROCMGR-6-PROCESS_STARTED: 'Xmpp' starting wit
h PID=4546 (PPID=4544) -- execing '/usr/bin/Xmpp'
```

Verify that the extension has been installed:

```
switch#show extensions
Name Version/Release Status RPMs
---------------------------------- ------------------------ ------ ----
SecurityAdvisory0005Patch.swix 1.0.0e.Ar/2506963.secAdvi A,I 1

A: available | NA: not available | I: installed | NI: not installed | F:forced
```

Step 4. At this point all existing Cli sessions should be restarted to use the fixed version of openssl when performing "copy" commands.

Notes:
RedHat released a tool to detect CCS vulnerabilities here: https://access.redhat.com/labs/ccsinjectiontest/ along with an offline script. On server features that this is tested against (for example, Capi) this will falsely report that they are affected on agents that are not running the patched version. This is because the script is looking for the alarm that occurs in patched versions. SSL Servers were never affected due to their running of pre-vulnerability code. If the agent is restarted after installing the extension (ex. via "agent Capi shutdown" "no agent Capi shutdown") the agent will load the new library which will return

alarms satisfying the script.

Step 5. Make the extension persist across reboots:

```
switch#copy installed-extensions boot-extensions
switch#show boot-extensions
SecurityAdvisory0005Patch.swix
```

Verification of the OpenSSL version after resolution:

```
switch#sh ver det | grep -i openssl
openssl 1.0.0e.Ar 2506963.secAdvisory0005.6
```

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