Server Automation Alert: SSL/TLS MITM Vulnerability

(June 18, 2014)

ACTION: Deploy the *SSL/TLS MITV Update* SRVA_00177
The information in this alert should be acted upon right away.

Change Table for this Document

Date	Change
June 18, 2014	Initial Release

Issue that Requires Attention

Transport Layer Security (TLS)/ Man-in-the-middle (MITM) Vulnerability

The TLS/MITM vulnerability is a crafted handshake MITM attack that can force OpenSSL SSL/TLS clients and servers to use weak keying material.

This attack:

- Decrypts and modifies traffic from the attacked client and server.
- Can only be performed between a vulnerable client and server.

Impact on SA

SA versions 10.0 and 10.01 are the only releases that are affected by this OpenSSL vulnerability, because of the OpenSSL versions they use (OpenSSL 1.0.1 and 1.0.2). Fixes are available for both these versions.

HPSA 10.00 and 10.01 use OpenSSL 1.0.1 and 1.0.2, and, as a result, they are the only SA releases that are vulnerable to this attack vector. The SA Software Repository Download Accelerator nginx web server is compiled against OpenSSL 1.0.1.

Note: There are 6 issues reported in https://www.openssl.org/news/secadv_20140605.txt, but only the issue that this paper addresses requires fixing in SA.

Immediate Mitigation

To make sure that this vulnerability will not affect SA, install the fixes for your system.

Apply the SA Software Repository Download Accelerator (Tsunami) – NGINX Fix

The *SA Software Repository Download Accelerator (Tsunami) – NGINX Update 06.14 (QCCR1D185866) (updated nginx binary OpenSSL 1.0.1h)* is a fix for the affected binary that was compiled with the vulnerable version of OpenSSL. The updated ngnix binary is now compiled against OpenSSL 1.0.1h.

To download and run the fix, go to:

http://support.openview.hp.com/selfsolve/document/LID/SRVA_00177

Note: The fix for the previously identified Heartbleed bug QCCR1D183160 / CVE-2014-0160 – the "Heartbleed" vulnerability found in impacted OpenSSL cryptographic software library is included with the new patch. **Customers should NOT install the "Heartbleed" fix after installing this MITM fix, since the Heartbleed fix will overwrite the MITM fix.**

Note: For SA versions 10.00 and 10.01, you must apply the fix to each slice on the SA Core. In addition, for SA 10.01, you must also apply the fix on each satellite server in the mesh. Contact HP Support for additional assistance.

Applying the Fix

To apply the fix, issue the following commands:

```
[root@dc1 ~]# tar -xvzf QC185866_10.01.NGINX_51064.tar.gz
[root@dc1 ~]# cd QC185866_10.01.NGINX_51064
[root@dc1 QC185866_10.01.NGINX_51064]# ./patch.sh -v install
```

After you apply the fix, the Accelerator starts automatically.

Verifying the Fix

To verify the fix, run the list open files (`lsof`) command and confirm that the results are as expected.

To run the `lsof` command:

```
[root@dc1 ~]# lsof -i:8061
```

The expected output of the `lsof` command (as the following example illustrates) will show that there are NGINX processes listening on port 8061:

```
COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME
nginx 7111 root 7u IPv4 17594 TCP *:8061 (LISTEN)
nginx 7112 root 7u IPv4 17594 TCP *:8061 (LISTEN)
nginx 7113 root 7u IPv4 17594 TCP *:8061 (LISTEN)
nginx 7115 root 7u IPv4 17594 TCP *:8061 (LISTEN)
nginx 7116 root 7u IPv4 17594 TCP *:8061 (LISTEN)
nginx 7117 root 7u IPv4 17594 TCP *:8061 (LISTEN)
nginx 7118 root 7u IPv4 17594 TCP *:8061 (LISTEN)
nginx 7119 root 7u IPv4 17594 TCP *:8061 (LISTEN)
nginx 7120 root 7u IPv4 17594 TCP *:8061 (LISTEN)
[root@dc1 ~]#
```

Note: Contact HP Support for additional assistance if your results are not similar to the example output.

For more details regarding the Heartbleed bug (CVE-2014-0160) see:
http://support.openview.hp.com/selfsolve/document/LID/SRVA_00174.