Server Automation Alert: Heartbleed OpenSSL Bug Vulnerability

(April 28, 2014)

ACTION: Deploy the *SA Software Repository Download Accelerator (Tsunami) - NGINX Update* SRVA 00174
The information in this alert should be acted upon right away.

Change Table for this Document

Date	Change
April 14, 2014	Initial Release
April 28, 2014	The *SA Software Repository Download Accelerator (Tsunami) – NGINX Update* fix is introduced. This fix modifies the SA Software Repository Download Accelerator component (also known as the Accelerator, or tsunami in this document) so that it is no longer vulnerable to the Heartbleed bug. After you run this update, the Accelerator becomes re-enabled, to benefit from the improved download performance it provides.

Issue that Requires Attention

The Heartbleed bug (**CVE-2014-0160**) is a vulnerability found in the OpenSSL cryptographic software library.

This vulnerability allows an attacker to:

- Steal the information typically protected by the SSL/TLS protocol.
- Read the memory of the systems using vulnerable versions of OpenSSL.
- Steal the SSL private key (used for SSL encryption) and therefore compromise all data encrypted by the key. Stealing the key allows attackers to eavesdrop on communications, steal data directly from the server, and impersonate services and end users.

You cannot verify, with 100% certainty, that your environment has not already been compromised.

Vulnerability Origin:

1. Direct use of affected OpenSSL version libraries
2. Web/Application servers using affected OpenSSL version libraries
3. Operating system that includes affected OpenSSL version libraries

Note: See also the following HPSW Security Bulletin:

https://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=emr_na-c04236102

Impact on SA

The SA Software Repository Download Accelerator component running on the following versions of SA component hosts is vulnerable to the Heartbleed bug:

- SA 10.00 and 10.01 slice servers
- SA 10.01 satellite servers

No other supported versions of SA are affected.

Note: In this document, the SA Software Repository Download Accelerator is referred to as “the Accelerator” or “tsunami.”

Immediate Mitigation

To make sure that the Heartbleed bug will not affect your SA System, complete the steps in the following sections:

- **Performing Pre-Update Steps**
- **Applying the SA Software Repository Download Accelerator (Tsunami) - NGINX Update**

Performing Pre-Update Steps

In the previous version of this memo, you were advised to disable the Accelerator to secure your environment against the Heartbleed bug. Disabling the Accelerator caused Software Repository downloads to bypass the Accelerator and revert to the traditional Software Repository access methods, which might result in slower performance, depending on the demands of your environment.

Disabling the Accelerator is no longer necessary. If you previously disabled the Accelerator, you must re-enable it to restore download performance in your SA environment.

Note: You only need to perform these pre-update steps if you already disabled the Accelerator, as the earlier version of this memo advised you to do.

Re-Enabling the Accelerator on SA 10.00 Cores

To re-enable the Accelerator on SA 10.00 Cores, issue the following commands:

```
# cd /etc/opt/opsware/startup
# mv tsunami.disabled tsunami
```

Re-Enabling the Accelerator on SA 10.01 Cores and Satellites

To re-enable the Accelerator on SA 10.01 Cores and Satellites, issue the following command:

```
# rm /var/opt/opsware/tsunami/tsunami.disabled
```

Applying the *SA Software Repository Download Accelerator (Tsunami) - NGINX Update*

The *SA Software Repository Download Accelerator (Tsunami) – NGINX Update (QCCR1D183160)* is a fix for the affected binary that was compiled with the vulnerable version of OpenSSL (1.0.1c). The updated nginx binary is now compiled against OpenSSL 1.0.1g

To download and run the fix, go to:
http://support.openview.hp.com/selfsolve/document/LID/SRVA_00174
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 QC183160_10.01.NGINX_49064.tar.gz
[root@dc1 ~]# cd QC183160_10.01.NGINX_49064
[root@dc1 QC183160_10.01.NGINX_49064]# ./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.

Stolen Private Key

If an attacker has already obtained the Software Repository component's wordbot private key, your SA environment can potentially be compromised.

Depending on your SA expertise, your SA environment, and the probability that the private key was compromised, you might consider performing the following additional actions:

- Reinstallation of your SA environment to regenerate the crypto material

  (Contact HP Support for additional assistance.)

- SA core recertification

  (Contact Support/CPE for assistance. Additional patches for SA and guidance will be required.)