HP BSAE Alert:
TLS SSL protocol Vulnerability CVE-2009-3555

Document Release Date: February 13, 2015
Affected Releases: 9.1x, 9.2x

ACTION: Use the instructions in this alert to update BSAE cores.
This information should be acted upon immediately.

Change Table for this Document

Date	Change
Feb 13, 2015	Initial Release

Issue that Requires Attention

CVE-2009-3555

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3555

Note: This link provides further information about this issue and lists the versions affected.

HP has investigated the CVE-2009-3555 vulnerability in relation to BSAE. This document provides required actions you must perform to mitigate this vulnerability.

Impact on BSAE

The Vulnerability is not limited to any specific software implementation, but is rather a fundamental protocol design flaw; a lot of software using SSL/TLS is vulnerable. For BSAE this includes the Java Secure Socket Extension (JSSE) component of Java Runtime Environment which is found to be vulnerable as explained in the Oracle documentation at the following link:

http://www.oracle.com/technetwork/java/javase/documentation/tlsreadme2-176330.html

Because BSAE 9.1x and 9.2x use JRE 6 Update 14, which is found to be a vulnerable JRE version, the different components of the bsae service listening on ports 8443 and 14445 are also vulnerable.

Immediate Mitigation Actions

To address this issue, the IETF TLS working group has defined a TLS protocol extension that allows safe session renegotiation. This protocol extension is described in RFC 5746, "Transport Layer Security (TLS) Renegotiation Indication Extension": **http://www.rfc-editor.org/rfc/rfc5746.txt**

Support for RFC 5746 in the Sun Java Runtime Environment (JRE) was introduced upstream in version 6 Update 22 to mitigate this flaw by disabling or limiting the use of renegotiation.

For more details on the renegotiation behavior in the patched Sun JRE, see:

http://www.oracle.com/technetwork/java/javase/documentation/tlsreadme2-176330.html

Perform the following actions on your BSAE core irrespective of the installation type (single or dual server).
No changes are need on the database server in case of Dual server.

1. Download the latest available Java Development Kit 6 binary for the x64 bit Linux architecture. As of this writing the latest binary available to download is JDK6 Update 45.

   http://download.oracle.com/otn/java/jdk/6u45-b06/jdk-6u45-linux-x64.bin

2. Copy the downloaded binary into a `/tmp` folder on the BSAE core server.
3. Install the binary. The installation will create the `jdk1.6.0_u45` folder under `/tmp` and extract the contents of the binary into the folder.

   ```
   # cd /tmp
   # chmod 0755 jdk-6u45-linux-x64.bin
   # ./ jdk-6u45-linux-x64.bin
   ```

4. Stop the BSAE and BSAE BO services.

   On BSAE 9.1x

   ```
   # /etc/init.d/opsware-omdb stop
   # /etc/init.d/bsae-bo stop
   ```

   On BSAE 9.2x

   ```
   # /etc/init.d/bsae stop
   ```

5. Remove existing `jdk1.6` folder.

   ```
   # rm -rf /opt/opsware/jdk1.6
   ```

6. Move `jdk1.6.0_u45` to `/opt/opsware/jdk1.6`.

   ```
   # mv /tmp/jdk1.6.0_45  /opt/opsware/jdk1.6
   ```

7. Start the BSAE and BSAE BO Service

   On BSAE 9.1x

   ```
   # /etc/init.d/bsae-bo start
   # /etc/init.d/opsware-omdb start
   ```

   On BSAE 9.2x

   ```
   # /etc/init.d/bsae start
   ```