BSAE Alert:
CVE-2015-4000: Logjam Vulnerability

Document Release Date: June 12, 2015
Affected Releases: All supported releases. (BSAE 9.10, 9.11, and 9.2)

ACTION: Update the BSAE core using the instructions in this document.

Issue that Requires Attention 2
Impact on BSAE 2
Immediate Mitigation 2
Appendix 4

Change Table for this Document

Date	Change
June 12, 2015	Initial Release

Issue that Requires Attention

Logjam Vulnerability: CVE-2015-4000

https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4000
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000

When a DHE_EXPORT cipher suite is enabled on a server but not on a client, the TLS protocol 1.2 and earlier does not properly convey a DHE_EXPORT choice. This allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE. This is known as the "Logjam" issue.

Impact on BSAE

The BSAE core is the platform management center for a BSAE system. It has a JBoss Application Server instance running necessary services.

Java Desktop clients interact with the BSAE core on port 14445. This JBoss AS port is configured for secured communication and allows usage of EXPORT ciphers by default.

All supported releases of BSAE are found to be vulnerable.

Immediate Mitigation

Verify and remove support for EXPORT ciphers in the BSAE core

The following changes needs to be performed on the BSAE core, irrespective of the installation type (Single or Dual server.) No changes are need on the database server in the case of a Dual server. Please note that HP Support can assist you with the following steps.

1. Log in to the BSAE core system as *root*.
2. Verify if EXPORT ciphers are supported in your BSAE core:

   ```
   # openssl s_client -connect localhost:14445 -cipher 'EXP'
   ```

   If you get a handshake failure error, then core is **NOT** vulnerable to the Logjam issue. EXPORT ciphers are not supported. You can skip further steps and **NO** action needed.

   If the connection is successful, the core is vulnerable and EXPORT ciphers are supported. Perform the remaining steps to disable EXPORT ciphers.
3. Stop the BSAE service on the core machine using one of the following commands, depending on your BSAE version:

   For 9.2:

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

   For 9.1x

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

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

4. Define the JRMP Invoker Service:

   a) Make a back-up of JBoss Service Configuration file:

   ```
   #  mkdir /var/tmp/CVE-2015-4000/
   #  cp /opt/opsware/omdb/omdb/conf/jboss-service.xml   /var/tmp/CVE-2015-4000/jboss-service.xml
   ```

   b) Comment out JRMPInvoker MBean from the original file (configured to listen at port 14445):

   ```
   # vi /opt/opsware/omdb/omdb/conf/jboss-service.xml
   ```

   ```
   <!--
       <mbean code="org.jboss.invocation.jrmp.server.JRMPInvoker"
          name="jboss:service=invoker,type=jrmp,socketType=SSL">
          <attribute name="RMIObjectPort">14445</attribute>
          <attribute name="ServerAddress">${jboss.bind.address}</attribute>
          <attribute name="RMIClientSocketFactory">org.jboss.security.ssl.RMISSLClientSocketFactory</attribute>
          <attribute name="RMIServerSocketFactory">org.jboss.security.ssl.RMISSLServerSocketFactory</attribute>
          <attribute name="SecurityDomain">java:/jaas/RMI+SSL</attribute>
          <depends>jboss.security:service=JaasSecurityDomain,domain=RMI+SSL</depends>
          <depends>jboss:service=TransactionManager</depends>
       </mbean>
   -->
   ```

   c) Copy the `jrmp-invoker-service.xml` file listed in the **Appendix** to the BSAE core.

      i. Use any text editor and create a new file named **jrmp-invoker-service.xml** under the deploy directory of the BSAE core:

      ```
      # vi /opt/opsware/omdb/omdb/deploy/jrmp-invoker-service.xml
      ```

      ii. Copy contents from the **Appendix** to the new file and save.

      iii. Change permissions of the`jrmp-invoker-service.xml` file to omdb:omdb:

      ```
      # chown omdb:omdb /opt/opsware/omdb/omdb/deploy/jrmp-invoker-service.xml
      ```

5. Start BSAE using one of the following commands, depending on your BSAE version:

   For 9.2:

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

   For 9.1x:

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

Appendix

File to be copied into the BSAE core - /opt/opsware/omdb/omdb/deploy/jrmp-invoker-service.xml

```
<?xml version="1.0" encoding="UTF-8"?>

<server>

<mbean code="org.jboss.invocation.jrmp.server.JRMPInvoker"
        name="jboss:service=invoker,type=jrmp,socketType=SSL">

    <attribute name="RMIObjectPort">14445</attribute>

    <attribute name="RMIClientSocketFactory">org.jboss.security.ssl.RMISSLClientSocketFactory</attribute>

    <attribute name="RMIServerSocketFactoryBean"
    attributeClass="org.jboss.security.ssl.RMISSLServerSocketFactory" serialDataType="javaBean">

        <property name="bindAddress">${jboss.bind.address}</property>

        <property name="SecurityDomain">java:/jaas/RMI+SSL</property>

        <property name="Protocols">SSLv2Hello,TLSv1</property>

        <property name="CiperSuites">
        TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES
        _128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_D
        HE_DSS_WITH_3DES_EDE_CBC_SHA</property>

    </attribute>

    <depends>jboss:service=TransactionManager</depends>

    <depends>jboss.security:service=JaasSecurityManager</depends>

</mbean>

</server>
```