# BSAE Alert:
# CVE-2013-2566: SSL RC4 Cipher Suites Supported

(April 22, 2015)

**ACTION**: Update BSAE core with the documented instruction.



**Effected Versions –** All supported releases (i.e.,) BSAE 9.10, 9.11 and 9.2

## Change Table for this Document

| Date | Change |
|---|---|
| **April 22, 2015** | Initial Release |
| | |

# Issue that Requires Attention

CVE-2013-2566: SSL RC4 Cipher Suites Supported

**http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566**
**http://www.tenable.com/plugins/index.php?view=single&id=65821**

The RC4 algorithm, as used in the TLS protocol and SSL protocol, has many single-byte biases, which makes it easier for remote attackers to conduct plaintext-recovery attacks via statistical analysis of cipher text in a large number of sessions that use the same plaintext.

# Impact on BSAE

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

This JBoss AS has a web container that is configured for secured communication on port 8443. Dataminer and Webclients such as browsers interact with BSAE core on this HTTPS port. This port currently allows usage of SSL RC4 cipher suites.

JBoss AS port 14445 is also configured for secured communication and allows usage of SSL RC4 cipher suites. Java Desktop clients interact with BSAE core using this port.

All supported releases of BSAE are found to be Vulnerable.

# Immediate Mitigation

**Remove SSL RC4 cipher support in BSAE core**

The following changes needs to be performed on the BSAE core, irrespective of the installation type (i.e., 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. Login to BSAE Core system as *root*.
2. 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
   ```

3. Disable the RC4 cipher suite on JBoss HTTPS port 8443:

   a) Make a back-up of the JBoss web container configuration file:

```
# mkdir /var/tmp/CVE-2013-2566

# cp /opt/opsware/omdb/omdb/deploy/jboss-web.deployer/server.xml
/var/tmp/CVE-2013-2566/server.xml
```

   b) Modify SSL enabled HTTP connector in the original file :

   */opt/opsware/omdb/omdb/deploy/jboss-web.deployer/server.xml*

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
"maxThreads="150" scheme="https" secure="true"
address="${jboss.bind.address}" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true"
ciphers="SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,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_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
securityDomain="java:/jaas/RMI+SSL" clientAuth="false"
sslProtocols="SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2"
SSLImplementation="org.jboss.net.ssl.JBossImplementation" />
```

   In the above connector configuration, remove SSL_RSA_WITH_RC4_128_MD5 and SSL_RSA_WITH_RC4_128_SHA ciphers.

   The updated configuration will be:

```
<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
"maxThreads="150" scheme="https" secure="true"
address="${jboss.bind.address}" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true"
ciphers="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_DHE_DSS_WITH_3DES_EDE_CBC_SHA"
securityDomain="java:/jaas/RMI+SSL" clientAuth="false"
sslProtocols="SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2"
SSLImplementation="org.jboss.net.ssl.JBossImplementation" />
```

4. Disable the RC4 cipher suite on JBoss port 14445:

   a) Check if SSL based JRMP invoker service is already defined:

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

   If **above file exists**, JRMP service is already defined. Perform steps listed in **4b (Update JRMP Invoker Service)** to update the service.

   If **there is no such file**, perform steps listed in **4c (Define JRMP Invoker Service)** to define this service.

   b) Update JRMP Invoker Service:

      I. Make a back-up of JRMP Invoker Service:

```
# cp /opt/opsware/omdb/omdb/deploy/jrmp-invoker-service.xml
   /var/tmp/CVE-2013-2566/
```

II. Update CipherSuites property of the Invoker Service:

*/opt/opsware/omdb/omdb/deploy/jrmp-invoker-service.xml*

```
<property name="CiperSuites">
SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_AES_1
28_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_DHE_DSS_WITH_3DES_EDE_CBC_SHA</property>
```

In the above property, remove SSL_RSA_WITH_RC4_128_MD5 and SSL_RSA_WITH_RC4_128_SHA ciphers.

The updated property will be:

```
<property name="CiperSuites">
TLS_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DH
E_DSS_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA
_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA</property>
```

III. Continue to step **5** for restarting the BSAE core.

c) Define JRMP Invoker Service

I. Make a back-up of JBoss Service Configuration file:

```
# cp /opt/opsware/omdb/omdb/conf/jboss-service.xml   /var/tmp/CVE-
2013-2566/jboss-service.xml
```

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

*/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>
-->
```

III. Copy jrmp-invoker-service.xml listed in Appendix (page **6**) to BSAE core.

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

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

ii. Copy contents from Appendix (page **6**) to the new file and save.

iii. Change permissions of the 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 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>
```

©Copyright 2015 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither HP or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice. Hewlett-Packard Company and the names of Hewlett-Packard products referenced herein are trademarks of Hewlett-Packard Company in the United States and other countries. Other product and company names mentioned herein may be trademarks of their respective owners.