

# BSAE Alert: POODLE: SSLv3 Vulnerability

---

(November 12, 2014)

**ACTION:** Update BSAE core with the documented instruction.  
The information in this alert should be acted upon right away.



Issue that Requires Attention .....2  
Impact on BSAE .....2  
Immediate Mitigation.....2

## Change Table for this Document

Date	Change
Nov 12, 2014	Initial Release

## Issue that Requires Attention

SSLv3 exposes vulnerability: [CVE-2014-3566](#)

The Poodle attack is a MITM (Man in the Middle) vector that allows an attacker to force a protocol downgrade between a client and server. This means both the client and the server must be able to communicate with this downgraded protocol.

## Impact on BSAE

### General

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 which is configured for secured communication on port 8443. Dataminer and Webclients such as browsers interact with BSAE core on this HTTPS port which currently allows SSLv3.

JBoss AS port 14445 is also configured for secured communication and allows SSLv3. Java Desktop clients interact with BSAE core using this port.

## Immediate Mitigation

### Remove SSLv3 support in BSAE core

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

1. Obtain the BSAE Hot Fix: jrmp-invoker-service.xml from HP Support.
2. Login to BSAE Core system as “root”
3. Stop BSAE service on the core machine:  
For 9.2  
`# /etc/init.d/bsae stop`  
For 9.1x  
`# /etc/init.d/opsware-omdb stop`  
`#/etc/init.d/bsae-bo stop`
4. Disable SSLv3 on JBoss HTTPS port 8443

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

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

- b) Modify SSL enabled HTTP connector in 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" sslProtocol="TLS"
SSLImplementation="org.jboss.net.ssl.JBossImplementation" />
```

In the above connector configuration:

- I. Remove: `sslProtocol="TLS"`
- II. Add: `sslProtocols="SSLv2Hello,TLSv1,TLSv1.1,TLSv1.2"`

Make sure the new attribute is `sslProtocols` (plural form) and not `sslProtocol`.

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="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" />
```

## 5. Disable SSLv3 on JBoss port 14445

- a. Create a back-up of JBoss Service Configuration file:

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

- b. 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>
```

-->

- c. Copy the jrmp-invoker-service.xml obtained from HP Support to JBoss deploy directory.  
# cp jrmp-invoker-service.xml /opt/opsware/omdb/omdb/deploy/  
# chown omdb:omdb /opt/opsware/omdb/omdb/deploy/jrmp-invoker-service.xml

## 6. Start BSAE

For 9.2

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

For 9.1x

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

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

©Copyright 2014 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.