BSAE Alert: CVE-2013-4810: JBoss Invoker servlets do not require authentication

(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-2013-4810: JBoss Invoker servlets do not require authentication

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4810
https://access.redhat.com/articles/545183

The CVE ID for this flaw - CVE-2013-4810 - refers to exposure of unauthenticated JMXInvokerServlet and EJBInvokerServlet interfaces in JBoss. A remote attacker could exploit this flaw to invoke MBean methods and run arbitrary code.

Impact on BSAE

BSAE Core is the platform management center for a BSAE system. It has JBoss Application Server 4.2.3 running necessary services. By default, JMXInvokerServlet and EJBInvokerServlet in this version of JBoss are exposed unauthenticated. This makes BSAE vulnerable.

All supported releases of BSAE are found to be vulnerable.

Immediate Mitigation

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 case of a dual server.

To eliminate the possibility of an exploit:

1. Log in to the BSAE core server as *root*.
2. Stop the BSAE service, 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. Backup configuration files from http-invoker and jboss-web.deployer components

   ```
   # mkdir /var/tmp/CVE-2013-4810-Servlets-Hotfix/
   # cd /var/tmp/CVE-2013-4810-Servlets-Hotfix/
   ```

```
# cp /opt/opsware/omdb/omdb/deploy/http-invoker.sar/invoker.war/WEB-
INF/web.xml .

# cp /opt/opsware/omdb/omdb/deploy/jboss-web.deployer/context.xml .
```

4. Update security-constraints of http-invoker application

```
/opt/opsware/omdb/omdb/deploy/http-invoker.sar/invoker.war/WEB-
INF/web.xml
```

a) Comment out <security-constraint>, <login-config> and <security-role> elements in above config file.

```
<!--
    <security-constraint>
          <web-resource-collection>
                ……
          </web-resource-collection>
          <auth-constraint>
                ……
          </auth-constraint>
    </security-constraint>
    <login-config>
          ……
    </login-config>
    <security-role>
          ……
    </security-role>
-->
```

b) Copy the following updated elements in to config file:

```
<security-constraint>
    <web-resource-collection>
          <web-resource-name>HttpInvokers</web-resource-name>
          <description>An example security config that only allows
    users with the role HttpInvoker to access the HTTP invoker
    servlets
          </description>
          <url-pattern>/restricted/*</url-pattern>
          <url-pattern>/EJBInvokerServlet/*</url-pattern>
          <url-pattern>/JMXInvokerServlet/*</url-pattern>
    </web-resource-collection>
```

```
      <auth-constraint>
         <role-name>AAA.admin</role-name>
         <role-name>AAA.user</role-name>
      </auth-constraint>
   </security-constraint>

   <login-config>
      <auth-method>BASIC</auth-method>
      <realm-name>hp-bsae</realm-name>
   </login-config>

   <security-role>
      <role-name>AAA.admin</role-name>
   </security-role>
   <security-role>
      <role-name>AAA.user</role-name>
   </security-role>
```

5. Disable the authenticator defined in jboss-web.

```
/opt/opsware/omdb/omdb/deploy/jboss-web.deployer/context.xml
```

Comment out the following Valve element that configures Authenticator for all applications in the JBoss instance.

```
<!--

<Valve
className="org.jboss.web.tomcat.security.ExtendedFormAuthenticator"
disableProxyCaching="false" securePagesWithPragma="false" />

-->
```

6. Configure Authenticator for http-invoker application.

Create the following context configuration file:

```
# vi /opt/opsware/omdb/omdb/deploy/http-invoker.sar/invoker.war/WEB-
INF/context.xml
```

Add following contents to the file and save:

```
<Context cookies="true" crossContext="true">

<Valve className="org.apache.catalina.authenticator.BasicAuthenticator"
disableProxyCaching="false" securePagesWithPragma="false"/>

</Context>
```

7. Configure Authenticator for jmx-console application.

   Create the following context configuration file

   ```
   # vi /opt/opsware/omdb/omdb/deploy/jmx-console.war/WEB-INF/context.xml
   ```

   Add following contents to the file and save:

   ```
   <Context cookies="true" crossContext="true">

   <Valve
   className="org.jboss.web.tomcat.security.ExtendedFormAuthenticator"
   disableProxyCaching="false" securePagesWithPragma="false"/>

   </Context>
   ```

8. Restart the BSAE service, 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
   ```

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.