IBM

IBM Community

Search

Profiles ▾   Communities ▾   Apps ▾

Wikis

⌶ This Wiki ▾   Search

IBM TRIRIGA

Log in to participate

▾ Tags   ?

Find a Tag

You are in: IBM TRIRIGA > IBM TRIRIGA Application Platform > Security > Jboss Security Remediation

Jboss Security Remediation

☺ | Updated April 2, 2014 by dmazzella | Tags: *None*

Page Actions ▾

There are two security issues with Jboss 5.1.0 involving the JMX Console[1] and the EJBInvoker[2]. For detailed information, please view the following vulnerability database sources links below:

http://www.osvdb.org/show/osvdb/97153
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4810
http://zerodayinitiative.com/advisories/ZDI-13-229/

================ PART 1 =========================

I. For JMX - there are two options.

Option 1. See the following site: https://community.jboss.org/wiki/SecureTheJmxConsole - we reference this in our installation docs: http://pic.dhe.ibm.com/infocenter/tivihelp/v49r1/index.jsp?topic=%2Fcom.ibm.tap.doc_3.3.1%2Fins_install%2Ft_ist_install_on_jboss_and_mss.html

- - - - - or - - - - - -

Option 2. The JMX-Console could be removed all together. This is done by going into the jboss-5.1.0.GA/server/all/deploy directory and delete both of the jmx* directory and xml. (jmx-console.war and jmx-invoker-service.xml)

For the JMXInvokerServlet, Edit jboss-5.1.0.GA/server/all/deploy/http-invoker.sar/invoker.war/WEB-INF/web.xml

Find and remove these three sections:

1. ......remove.........

```
<servlet>
  <servlet-name>JMXInvokerServlet</servlet-name>
  <description>The JMXInvokerServlet receives posts containing serlized
    MarshalledInvocation objects that are routed to the invoker given by
    the the MBean whose object name hash is specified by the
    invocation.getObjectName() value. The return content is a serialized
    MarshalledValue containg the return value of the inovocation, or any
    exception that may have been thrown.
  </description>
  <servlet-class>org.jboss.invocation.http.servlet.InvokerServlet</servlet-class>
  <load-on-startup>1</load-on-startup>
</servlet>
```

2. ......remove.........

```
<servlet-mapping>
  <servlet-name>JMXInvokerServlet</servlet-name>
  <url-pattern>/JMXInvokerServlet/*</url-pattern>
</servlet-mapping>
```

3. ....remove.........

```
<servlet-mapping>
  <servlet-name>JMXInvokerServlet</servlet-name>
  <url-pattern>/readonly/JMXInvokerServlet/*</url-pattern>
</servlet-mapping>
```

================ PART 2 =========================

II . For EJBInvoker

Edit jboss-5.1.0.GA/server/all/deploy/http-invoker.sar/invoker.war/WEB-INF/web.xml
Find and remove these two sections:

1. .... remove ....

```
<servlet>
    <servlet-name>EJBInvokerServlet</servlet-name>
    <description>The EJBInvokerServlet receives posts containing serlized
    MarshalledInvocation objects that are routed to the EJB invoker given by
    the invokerName init-param. The return content is a serialized
    MarshalledValue containg the return value of the inovocation, or any
    exception that may have been thrown.
    </description>
    <servlet-class>org.jboss.invocation.http.servlet.InvokerServlet</servlet-class>
    <init-param>
        <param-name>invokerName</param-name>
        <param-value>jboss:service=invoker,type=http</param-value>
        <description>The RMI/HTTP EJB compatible invoker</description>
    </init-param>
    <load-on-startup>1</load-on-startup>
</servlet>
```

2. ....remove ....

```
<servlet-mapping>
    <servlet-name>EJBInvokerServlet</servlet-name>
    <url-pattern>/EJBInvokerServlet/*</url-pattern>
</servlet-mapping>
```

| **Comments (0)** | Versions (3) | Attachments (0) | About |

There are no comments.

🔲 Feed for this page | Feed for these comments

▶ **Members** ?