Securing JBoss Web Console JMX Invoker in Digitool

Overview

A remote unauthenticated attacker can use the Web Console's JMX Invoker to perform management tasks using the MBean interfaces that are available in the underlying JBoss installation. A zip file is attached to the article with the instructions necessary to mitigate this vulnerability, and includes configuration files which need to be added.

Goal - Secure the JBOSS (JMX) web console invoker in Digitool

The JBOSS deploy path can be located on the Digitool server
At the console type:
`>jb_deploy`
This will change to the deploy directory. Eg.:
`/exlibris/dtl/j3_1/digitool/home/system/thirdparty/openserver/server/default/deploy`
You will need to adjust this path if it differs from these instructions.

Implement the fix

Step 1 - Remove http-invoker.sar

Remove http-invoker.sar/ from the deploy path.

It is not sufficient to change the name it must be either deleted or moved outside the deploy path, eg. to /tmp

Step 2 - Download this file from the Digitool server to your PC

`/exlibris/dtl/j3_1/digitool/home/system/thirdparty/openserver/server/default/deploy/management/web-console.war`
Extract the following two files from web-console.war (*using Total Commander for example or other archive extractor*) and edit as follows:

WEB-INF/web.xml
Uncomment the security-constraint block and add a <login-config> block after the end of the <security-constraint> block *(if not already present).*

```
 <security-constraint>
   <web-resource-collection>
   <web-resource-name>HtmlAdaptor</web-resource-name>
   <description>An example security config that only allows users with the
```

```
role JBossAdmin to access the HTML JMX console web application
</description>
<url-pattern>/*</url-pattern>
<http-method>GET</http-method>
<http-method>POST</http-method>
</web-resource-collection>
<auth-constraint>
<role-name>JBossAdmin</role-name>
</auth-constraint>
</security-constraint>


<login-config>
   <auth-method>BASIC</auth-method>
   <realm-name>JBoss WEB Console</realm-name>
</login-config>
```

(Find example of this file in secure_web-invoker.zip attached to article)

WEB-INF/jboss-web.xml

Uncomment the security-domain block. Make sure the JNDI name maps to the realm name (e.g. JMXConsole)

```
<security-domain>java:/jaas/web-console</security-domain>
```

(Find example of this file in secure_web-invoker.zip attached to article)

Replace the files in web-console.war on the Digitool server with the edited versions.

Step 3 - Copy directory

In secure_web-invoker.zip you will find a directory “props”.
Copy it to this path on the Digitool server:
/exlibris/dtl/j3_1/digitool/home/system/thirdparty/openserver/server/default/conf/props

Step 4 - Edit this file

`/exlibris/dtl/j3_1/digitool/home/system/thirdparty/openserver/server/default/conf/login-config.xml`

Change the path in these sections to the versions in the new “props” directory by adding “props/” to the front of the path:

```
<application-policy name = "jmx-console">
            <authentication>
                  <login-module
                        code="org.jboss.security.auth.spi.UsersRolesLoginModule" flag =
                        "required">
                        <module-option name="usersProperties">
                              props/jmx-console-users.properties</module-option>
                        <module-option name="rolesProperties">
                              props/web-console-roles.properties</module-option>
                  </login-module>
            </authentication>
```

```
</application-policy>


<application-policy name = "web-console">
	<authentication>
		<login-module
			code="org.jboss.security.auth.spi.UsersRolesLoginModule" flag =
			"required">
			<module-option name="usersProperties">
				props/web-console-users.properties</module-option>
			<module-option name="rolesProperties">
				props/web-console-roles.properties</module-option>
		</login-module>
	</authentication>
</application-policy>
```

(Find example of this file in secure_web-invoker.zip attached to article)

Step 5 – Stop and start JBOSS

```
$jdtlh_bin/jboss_shutdown.sh
$jdtlh_bin/jboss_startup.sh
```

Attachment

Download secure_web-invoker.zip from this link: