【已复现】百度网盘远程命令执行漏洞POC及一键部署环境

漏洞介绍

近期在百度网盘 **Windows 客户端** 中被发现一处严重的 **远程命令执行（RCE）漏洞**。该漏洞源于客户端默认安装的服务程序在本地开启并监听TCP 10000 端口，通过HTTP 协议处理外部请求，但未对传入参数进行严格校验，攻击者可通过构造恶意请求触发命令执行，从而在受害者主机上获取系统权限，造成严重的安全风险。

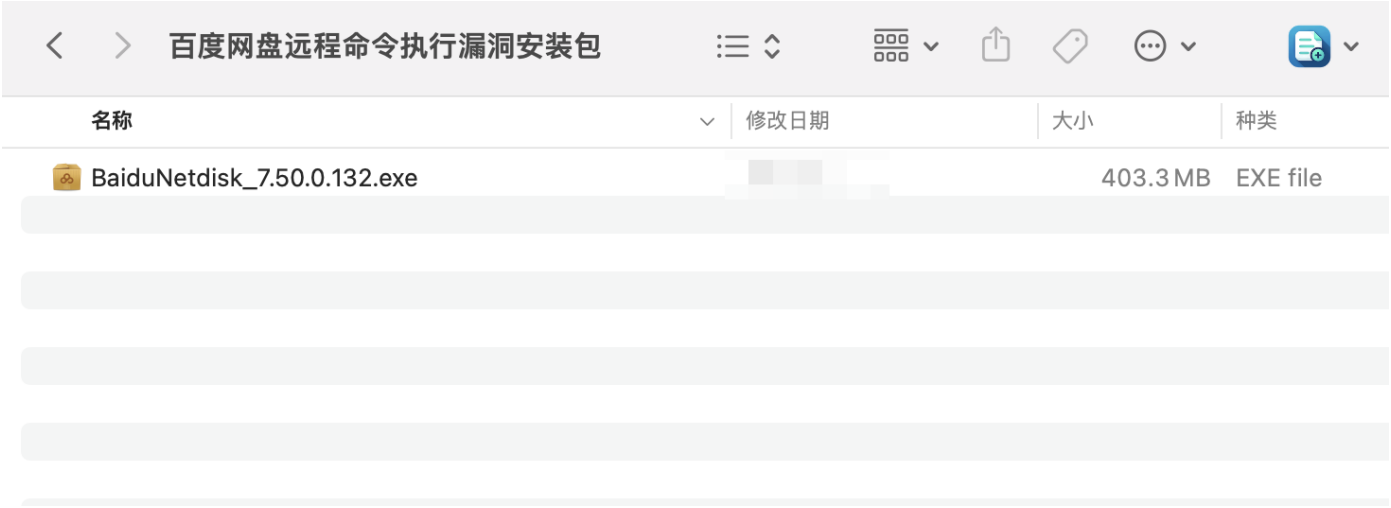
漏洞利用条件

- 百度网盘版本小于7.60.5.102
- 需要知道目标的windows用户名

漏洞环境部署

双击百度网盘安装包进行安装即可

> 相关安装包可在知识星球内领取，知识星球介绍详见文末



漏洞利用

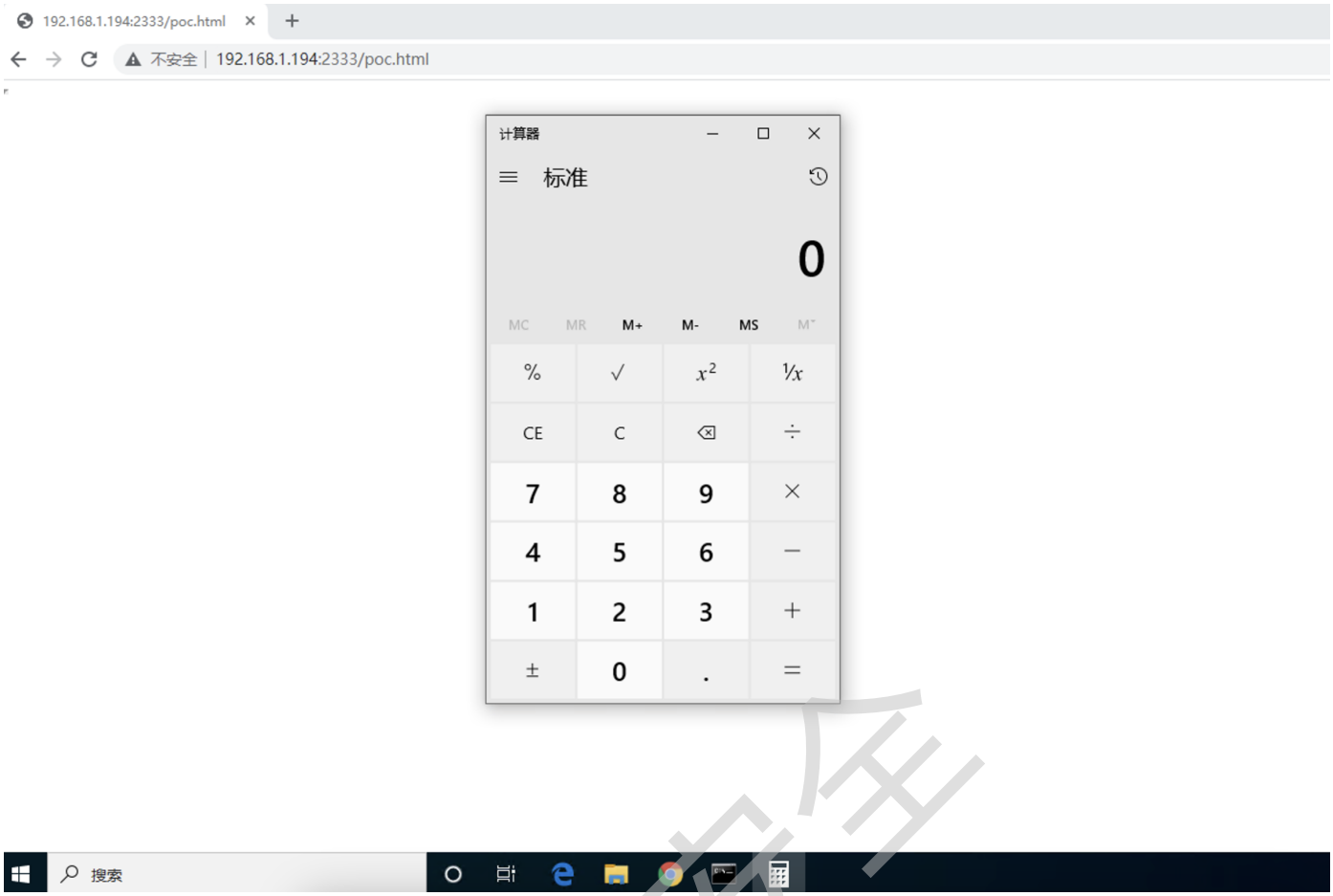
首先将两个POC：poc.html和poc.xml放在攻击机的同一个文件夹中，并开启一个http服务使得受害机能够访问到

> poc.html和poc.xml可在知识星球内领取，知识星球介绍详见文末

```
┌──(root㉿kali)-[~/BaiduYunPOC]
└─# ls
poc.html  poc.xml

┌──(root㉿kali)-[~/BaiduYunPOC]
└─# python3 -m http.server 2333
Serving HTTP on 0.0.0.0 port 2333 (http://0.0.0.0:2333/) ...
```

接着使用钓鱼、社会工程学等手法诱使受害者访问到poc.html网页即可出发远程命令执行漏洞（这里为了证明能够执行任意命令，弹出计算器；实际可将calc.exe替换为任意可执行命令）



漏洞修复

修复需要将版本升级

- 将百度网盘版本升级到7.60.5.102版本及以上
- 更新地址：https://pan.baidu.com/download#pan