sambaCry 漏洞复现

李昊清，何陈溪

复现过程

环境搭建

我们使用 vulhub 复现 smbd 4.6.3 的环境。vulhub 集成了 CVE-2017-7494 的 docker 环境，切换路径到 `vulhub/samba/CVE-2017-7494`，执行 `docker-compose up -d` 即可启动 samba server。

通过配置 `docker-compose.yml` 文件将 samba 共享路径映射到 server 路径，并设置可写权限，即满足漏洞利用的条件。

exploit

使用 metasploit 的 `linux/samba/is_known_pipename` 模块进行漏洞利用。设置 `RHOST` 和 `SMB_FOLDER`，成功拿到了 root shell

漏洞分析

`rpc_server/srv_pipe.c` 中的存在一个验证 BUG，攻击者可以利用客户端上传恶意动态库文件到具有可写权限的共享目录中，之后发出请求，使服务器加载 Samba 运行目录以外的非法模块，导致恶意代码执行。[1]

patch

github.com/samba-team/samba/commit/04a3ba4dbcc4be0ffc706ccc0b586d151d360015

[1] blog.csdn.net/weixin_45209963/article/details/129855384

在这里可以看到，pipename 的字符串被直接用来 `dlopen`，在后面被直接调用 `SAMBA_INIT_MODULE` 函数，如果攻击者成功上传自定义动态库，sambda 会直接执行任意函数

注：`dlopen` 和 `dlsym` 是系统调用 `shl_load` 和 `shl_findsym` 的简单封装，用于动态链接库的加载和函数的查找。

exp

1. smb_login 完成认证后，通过 simple.connect 建立连接，然后通过 simple.client.find_first 枚举所有路径，过滤出所有子 dir
2. 生成并上传一个随机的.txt 文件验证 w 权限
3. 找到 uri 对应在 remote 系统内的 path
4. 遍历所有 arch 的预先写好的 template，上传并尝试创建 named_pipe 触发漏洞，若 PIPE 报错值为 STATUS_OBJECT_PATH_INVALID 则执行成功