OS X/iOS 磁盘镜像子系统 UAF 漏洞分析

译者：布兜儿(看雪 ID：我有亲友团)

原文链接：https://bugs.chromium.org/p/project-zero/issues/detail?id=833

原文作者：ianbeer@google.com

CoreStorage 中的 OS X 内核 UAF 漏洞分析

在没有获得引用的情况下，CoreStorageUserClient 在+0xE0 区域通过 IOServiceOpen 存储了一个任务结构指针。

通过 kill 这个任务，我们可以释放掉这个指针，从而为用户端留下一个挂起指针。

有趣的地方在于，CoreStorageUserClient 将会使用这个悬挂指针来调用 IOUserClient::clientHasPrivilege 进行权限检查。所以如果我们可以得到这个原本由 root 权限的进程创建而后被释放掉的 task struct，我们就可以骗过这个检查，使其相信我们就是 root。想必他们要做的很多有趣的东西都被限制为 root 用户，比如混淆卷信息。

你也可以利用这个 bug 引发内核内存崩溃。

build: clang -o corestorage_task_uaf corestorage_task_uaf.c -framework IOKit

你应该设置 gzalloc_min=1024，gzalloc_max=2048 或者类似于 UAF 的实际错误，否则可能会得到一些奇怪的崩溃。

已在 MacBookAir5,2 ，OS X 10.11.5（15F34）上测试。