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=832

原文作者：ianbeer@google.com

微信公众号：看雪 iOS 安全小组 我们的微博：weibo.com/pediyiosteam

我们的知乎：zhihu.com/people/pediyiosteam

OS X/iOS 磁盘镜像子系统 UAF 漏洞分析

在没有获得引用的情况下，IOHDXIControllerUserClient 在 +0x1f8 地址通过 IOServiceOpen 存储了一个任务结构指针。

通过 kill 这个任务，我们可以释放这个指针，从而为用户端留下一个挂起指针。通过调用 CreateDrive64 外部方法，我们可以得到这个指针，这个方法将会试图读取和利用这块已被释放的任务结构的内存区域。

这个 bug 可以用于引发内存崩溃。

build: clang -o iohdix_task_uaf iohdix_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。