IOThunderboltFamily 中的 OS X 内核 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=834

原文作者：ianbeer@google.com

IOThunderboltFamily 中的 OS X 内核 UAF 漏洞分析

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

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

IOThunderboltFamilyUserClient 使用这个挂起指针来创建可读写的 IOMemoryBuffers（假设它可以读写被调用进程的任务）。通过重新分配一个带有权限进程的 task struct 结构体，以此覆盖被释放掉的那个结构体，我们可以得到 IOThunderboltFamilyUserClient 来造成内存崩溃。

你也可以利用这个 bug 引发内核内存崩溃。

build: clang -o thunderbolt_task_uaf thunderbolt_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。