# IOSurface 中的 OS X/iOS 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=831

**原文作者：ianbeer@google.com**

# IOSurface 中的 OS X/iOS 内核 UAF 漏洞分析

在没有获得引用的情况下，IOSurfaceRootUserClient 在 +0xf0 地址通过 IOServiceOpen 存储了一个任务结构指针。

通过 kill 相应的任务，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。

通过调用 create_surface_fast_path 外部方法我们可以得到这个指针，这个方法将会尝试读取和使用这块已被释放的任务结构的内存映射。

这个 bug 可以被用来引发内核内存崩溃，这可以通过一些有趣的沙箱比如 safari 或者 chrome 来实现。

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

你要设置 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。