launchd 中虚拟磁盘挂载尺寸分配问题导致 UAF

译者：赤(看雪 ID：呜呼哀哉)

原文链接：https://bugs.chromium.org/p/project-zero/issues/detail?id=896

原文作者：ianbeer@google.com

2016 年 八月二十二日 星期一

launchd 进程在 0x10000420D（10.11.6）处的 function 自动生成 MIG 代码, msgh_id 437 是由其解析而来。

虽然此 mig 方法采用了 out-of-line-ports 描述符，但是这个代码并没有校验 request_fdsCnt 是否等于实际描述符的大小，而且它使用了不受信任的方法去调用 mig_deallocate 来回收内存。

我们可以在它们运行过程中，通过传递一个较大的值来让后续页面被销毁。

这个 bug 可以在 OS X / iOS 中任意的沙箱发生。

如果想要真正的看到这个崩溃，首先你要在一个循环中跑这个 POC，然后做一些会导致很多 launchd 流量的事，比如：

在一个终端：while true; do ./legacy_ipc; done

在另一个终端：while true; do /Applications/Safari.app/Contents/MacOS/Safari& sleep 0.4 && killall Safari; done

测试是基于 MacBookAir5,2 上的 OS X 10.11.6（15G31）进行。