launchd 中消息队列逻辑问题允许任意的 mach message 控制

2016 年 八月二十日 星期六

Launchd 升级为 10.10 版本。旧版本的（10.10 之前）launchd 是开源的，但是新的版本是封闭源、被剥离出来的单独版本，所以甚至没有 function 名字

然而...

新版本的 launchd 与 xpc 的事物紧密集成,这样就给了我们一个良好的着力点去了解发生了什么。此 PoC 中的所有 function 地址均基于 OS X 10.11.6 装载的 launchd。

10002F3A1 是引导端口上的处理程序 - 当接收到消息时，它从 libxpc 中调用 xpc_pipe_try_receive，用来检查接收的 mach message 的 msgh_id：如果它是 0x10000000，那么这是一个 xpc message，它会尝试反序列化一个 xpc 对象；如果它是一个旧版本的 MIG message,则 xpc_pipe_try_receive 将调用其第 4 个参数通过 xpc_pipe_handle_mig 来处理 MIG 消息。 10002ED33 是 launchd 进程的旧版本的 mig 处理程序，它通过在 100018ADE 中注册的几个旧版本 MIG 子系统来进行检验（请注意，对 10002E3EE 的调用是指添加了旧版本的 mig 子系统到它们的数组。）（100018ADE 还注册了 launchd 的 XPC 子系统（ipc 系列）的处理程序）。

这是很好的，但有趣的是，实际上存在两个调用路径，一个是到 xpc_demuxer（10002EE87）/ mig 处理程序（10002ED33），而另一个是 10002EC25。除了不存在对 xpc_pipe_try_receive 的调用，此 function 的逻辑与 10002F3A1 几乎相同。稍稍回顾一下可以发现，当邮件由 launchd 接收时，此 function 不负责直接解析信息，而是用于“重新解析”“搁置”信息。

在某些情况下，当 launchd 无法立即服务请求时，它会将此请求排入调度队列稍后再试，并且该请求最终将在此处结束。

此 function（10002EC25）只直接接受 xpc dictionary，而且它会通过检查来发现该 dictionary 是否具有“mig-request” key/value pair。如果有，则它会在 xpc_dictionary 之外读取一个 xpc_data_t 并将其转换成一个 mach_msg_header_t，并将其通过 xpc_pipe_handle_mig 来传递到 10002ED33（旧版本 MIG 处理程序）。

我找不到任何可以设置一个“mig-request”值的地方，所以我猜这是一个调试功能，又或者是因为意外留下？因为 xpc 是一个无模式的 ipc 机制，我们实际上可以只设置一个具有完全受控制的 xpc_data_t 有效负载的“mig-request”键（其值将被视为被 launchd 接收的有效的 mach message）。唯一的先决条件是，我们要找出如何获取一个我们发送到 launchd 的被搁置的 XPC 信息的方法——而似乎子系统 3 的例程 804（xpc_look_up_endpoint）有时将被搁置，这意味着如果我们修改这些请求中的一个，我们可以通过旧版本的 MIG 处理管道发送一个完全受控制的伪造的 mach message。

这是一个惊人的野生的 exploitation ——当伪造的 mach message 能够传递到 mach_msg_destroy 来摧毁它的权限和内存时，这个 PoC 会发送一个带有 OOL 数据的信息，而这会导致读取一个在 0x414141410000 的内核端口成为一个崩溃的尝试（这个指针稍后也会被传递到 vm_deallocate）。但是一个像这样的 bug 可以使你做更多的事，例如扰乱 launchd 的端口的引用计数（因为我们可以在我们的信息中指定任意端口号，使其被看作是 launchd 的端口命名空间中的有效端口）。我们还可以取消映射任意页面，并将无效的事物传递给传统 MIG 处理程序。

就影响方面而言，launchd 是系统上权限最大的进程，你可以从任何进程涉及到它:-)

这个 PoC 会 hook 目标 xpc 请求的发送，并注入一个“mig-request”xpc_data_t —— 如果它不工作，尝试关闭所有打开的浏览器，或使用干净的启动重新开始。

译者：赤（看雪 ID:呜呼哀哉）

原文链接：**https://bugs.chromium.org/p/project-zero/issues/detail?id=893**

原文作者：ianbeer@google.com