黑云压城城欲摧 - 2016年iOS公开可利用漏洞总结

阿里聚安全 / 2016-12-27 06:37:16 / 浏览数 2863 安全技术 漏洞分析 顶(0) 踩(0)

黑云压城城欲摧 - 2016年iOS公开可利用漏洞总结
作者：蒸米，耀刺，黑雪 @ Team OverSky

0x00 序
iOS的安全性远比大家的想象中脆弱，除了没有公开的漏洞以外，还有很多已经公开并且可被利用的漏洞，本报告总结了2016年比较严重的iOS漏洞（可用于远程代码执行或

0x01 iOS 10.1.1 公开的可利用漏洞

1. mach_portal攻击链：该攻击链是由Google Project Zero的Ian
   Beer公布的。整个攻击链由三个漏洞组成:损坏的内核port的uref可导致任意进程的port被越权替换（CVE-2016-7637），powerd任意port替换可导致DoS（CVE-2016

攻击者先使用CVE-2016-7637将launchd与"com.apple.iohideventsystem"系统服务具有发送权限的port替换成自己控制的进程的port，并攻击者还具有该port的接收权限
port发送给了这个系统服务。但因为攻击者利用之前的CVE-2016-7637漏洞获取了"com.apple.iohideventsystem"系统服务port的接收权限，因此攻击者获得了powerd的
port，从而控制了具有root权限并且在沙盒外的powerd进程。攻击者随后利用powerd进程的task port获取到了host_priv port，然后利用host_priv
port触发因set_dp_control_port没有上锁而导致的XNU内核UaF（CVE-2016-7644）漏洞，从而控制了kernel task port。攻击者在获取了kernel
task以后，就可以利用系统提供的mach_vm_read()和mach_vm_write()去进行任意内核读写了。

2016年12月22日，qwertyoruiop在Ian
Beer公布的mach_portal攻击链的基础上，加入了KPP的绕过、内核patch和cydia的安装，并在自己的twitter上发布了iOS 10.1.*的越狱。

0x02 iOS 9.3.4 公开的可利用漏洞

1. PEGASUS
   三叉戟攻击链：该攻击链是在对阿联酋的一位人权活动家进行apt攻击的时候被发现。整个攻击链由三个漏洞组成：JSC远程代码执行（CVE-2016-4657），内核信息泄

在浏览器漏洞方面，由于iOS系统的JavaScriptCore库的MarkedArgumentBuffer类在垃圾回收的时候可能会造成内存堆破坏，导致黑客可以使用该漏洞泄露对象地址以及执
X
10.11.6本地提权：https://jaq.alibaba.com/community/art/show?articleid=531）。利用该攻击链可以做到iOS上的远程完美越狱，可以说是近几年来影响最大的iOS漏

利用PEGASUS对iOS 9.3.* 32位设备越狱的DEMO：http://v.youku.com/v_show/id_XMTg4NzA5OTEwOA==.html

0x03 iOS 9.3.3 公开的可利用漏洞

1. IOMobileFramebuffer Heapoverflow 内核漏洞:
   该漏洞存在于IOMobileFramebuffer这个内核服务中。在IOMobileFramebuffer::swap_submit(IOMFBSwap
   *)这个函数中，因为没有对用户态传入的IOMFBSwap数据进行校验，从而导致内核堆溢出。利用该漏洞可以在沙盒内（不需要沙盒逃逸）直接对内核进行攻击，并完成非
   9.3.3盘古越狱(女娲石)中被使用。

0x04 iOS 9.3.2 公开的可利用漏洞

1. WebKit RCE heapPopMin 远程代码执行漏洞: 因为Webkit模块中的WebCore
   ::TimerBase::heapPopMin()存在内存破坏漏洞，利用该漏洞可以对iOS设备进行远程攻击。当用mobile
   safari浏览有恶意攻击代码的网页的时候，safari将会被黑客控制。但要注意的事，被控制的仅仅是safari，想要获取用户数据还需要进行沙盒逃逸，想要控制手机还需要对
1. GasGauge 条件竞争内核漏洞:
   该漏洞存在于GasGauge这个内核服务中，因为在free内存的时候没有进行加锁操作，黑客可以开多个线程进行free操作，当竞争成功的时候可以造成double
   free的漏洞，随后可以转化为任意zone的UAF并控制内核，并完成非完美越狱。需要注意的是，该内核服务并不能在沙盒内直接访问，所以想要利用该漏洞，需要先做到

0x05 iOS 9.3.1 公开的可利用漏洞

1. inpuTbag Heapoverflow 内核漏洞: 该漏洞是阿里移动安全的OverSky团队发现并公布的，该漏洞存在于IOHIDDevice这个内核服务中，因为没有对Input
   report的szie做检测从而造成内核堆溢出。利用该漏洞可以对内核进行攻击，并完成非完美越狱。需要注意的是，该内核服务需要在沙盒外并拥有"com.apple.hid.manag

0x06 iOS 9.1 公开的可利用漏洞

1. CVE-2015-7037 Photos 沙盒逃逸漏洞:
   该漏洞存在于com.apple.PersistentURLTranslator.Gatekeeper这个系统服务中，在盘古越狱中被使用，通过利用改漏洞，一个在沙盒内的app可以做到mobile权限的沙
1. CVE-2015-7084 IORegistryIterator 内核漏洞:
   该内核漏洞存在于IOKit中，因为IORegistryIterator对象没有线程互斥的保护，导致对成员进行操作的时候可能出现错误。该漏洞可以在沙盒内直接通过race
   condition触发, 随后转化为内核信息泄露以及内核的代码执行，并做到非完美越狱。

0x07 iOS 9.0 公开的可利用漏洞

1. CVE-2015-6974 IOHIDFamily 内核漏洞：该漏洞存在于IOHIDResource这个内核服务中，在terminateDevice后，系统没有将device设置为NULL,
   从而造成UAF漏洞。该漏洞在盘古iOS
   9.0越狱中被使用，利用该漏洞可以做到内核的任意读写，并完成非完美越狱。需要注意的是，该内核服务并不能在沙盒内直接访问，所以想要利用该漏洞，需要先做到沙

0x08 总结

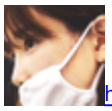
可以看到2016年的公开可利用的漏洞数量是非常巨大的，相对2015年可以说是有了一个指数级的增长。虽然苹果更新系统的速度非常快并且无法降级，但随着老设备（iPho
4s及以下已无法升级iOS 10）越来越多，并且用户对新系统期望越来越低，iOS设备的更新率已经变得非常缓慢。

根据某专业移动分析平台2016年12月的数据可以看到，仅有3.28%的设备更新了最新版的iOS
10.2。这意味着96.72%的设备都有被最近刚发布的mach_portal漏洞攻击的风险。我们相信，在新的一年，iOS的漏洞数量还会持续增加，并且随着漏洞利用技术的公开，

最后，对本文提到的漏洞感兴趣的同学可以在我们的github上学习相关的资料：https://github.com/zhengmin1989/GreatiOSJailbreakMaterial

上一篇：Apache Tomcat的安全相关东西 下一篇：攻击JavaWeb应用[4]-SQ...

1. 2 条回复


hades 2016-12-29 13:54:08

下一篇是不是2016安卓版本？

0 回复Ta


笑然 2016-12-30 09:21:36

总将得很棒

0 回复Ta
