OSX/IOS 系统漏洞学习资料汇总

pandazheng

随着 OSX/IOS 系统的不断普及，相信在未来 OSX/IOS 安全性也会受越来越多的人关注，今天有时间我就把自己学习的一些 OSX/IOS 系统漏洞的资料总结一下，方便自己和爱好这方面的人一起研究学习，路漫漫其修远兮 吾将上下而求索！

OSX/IOS 漏洞集合网站：
https://www.exploit-db.com/platform/?p=osx
https://www.exploit-db.com/platform/?p=ios
https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-15556/Apple-Iphone-Os.html
http://www.macexploit.com/

OSX/IOS 漏洞研究博客：
Hidden backdoor API to root privileges in Apple OS X
https://truesecdev.wordpress.com/2015/04/09/hidden-backdoor-api-to-root-privileges-in-apple-os-x/
Metasploit post exploitation scripts to steal ios5 backups
http://www.securitylearn.net/2012/09/09/metasploit-post-exploitation-scripts-to-steal-ios-5-backups/
OS X 10.10 DYLD_PRINT_TO_FILE Local Privilege Escalation Vulnerability
https://www.sektioneins.de/en/blog/15-07-07-dyld_print_to_file_lpe.html
Researchers discover new keychain vulnerability in osx
http://www.csoonline.com/article/2979068/vulnerabilities/researchers-discover-new-keychain-vulnerability-in-osx.html
Drop-dead simple exploit completely bypasses Mac’s malware Gatekeeper
http://arstechnica.com/security/2015/09/drop-dead-simple-exploit-completely-bypasses-macs-malware-gatekeeper/
IOS9.2/9.2.1 修补的内核漏洞
http://blog.pangu.io/race_condition_bug_92/
POC2015 & RUXCON2015 盘古团队议题
http://blog.pangu.io/poc2015-ruxcon2015/
一个“短命”的 IOS 内核漏洞
http://blog.pangu.io/short-lifecycle-bug/
IOS8.4.1 Kernel Vulnerabilities in AppleHDQGasGaugeControl
http://blog.pangu.io/ios-8-4-1-kernel-vulns/
CVE-2015-5774
http://blog.pangu.io/cve-2015-5774/
IOS8.1.2 越狱过程详解及相关漏洞分析
http://nirvan.360.cn/blog/?p=887
从 p0sixspwn 源码看越狱流程，原理，目的

http://bbs.pediy.com/showthread.php?t=193859&viewgoodnees=1&prefixid=
Pangu8 越狱中所用/usr/libexec/neagent 漏洞原理分析
http://bbs.pediy.com/showthread.php?t=195495&viewgoodnees=1&prefixid=
DYLD_ROOT_PATH dyld 本地提取漏洞分析
http://nirvan.360.cn/blog/?p=455
tpwn 分析
http://nirvan.360.cn/blog/?p=469
CVE-2015-5774 分析及利用
http://nirvan.360.cn/blog/?p=461
CVE-2014-4423 分析过程及结论
http://nirvan.360.cn/blog/?p=450
IOS ODay 分析：播放视频造成内核 DoS
http://nirvan.360.cn/blog/?p=487
IOS 进程通讯安全和利用
http://nirvan.360.cn/blog/?p=723
在非越狱的 iPhone6(IOS8.1.3)上进行钓鱼攻击（盗取 App Store 密码）
http://drops.wooyun.org/mobile/4998
IOS URL Scheme 劫持-在未越狱的 iPhone6 上盗取支付宝和微信支付的帐号和密码
http://drops.wooyun.org/papers/5309
IOS 冰与火之歌-Object-C Pwn and IOS arm64 ROP
http://drops.wooyun.org/papers/12355
IOS 冰与火之歌-在非越狱手机上进行 App Hook
http://drops.wooyun.org/papers/12803
对 dyld 的分析（源码，代码签名等）
http://cocoahuke.com/2016/02/14/dyld%E5%8A%A0%E8%BD%BD%E8%BF%87%E7%A8%8B/
太极 taiji(IOS8.4)Info 和部分反编译代码
http://cocoahuke.com/2015/09/18/taij(iOS8.4)/
CVE-2015-5774
http://cocoahuke.com/2015/09/18/describeCVE-2015-5774/

OSX/IOS 漏洞源码：
https://github.com/tihmstar/rootpipe_exploit
https://github.com/jndok/ropnroll
https://github.com/tyranid/canape-ssl-mitm-osx
https://github.com/kpwn/vpwn
https://github.com/kpwn/tpwn
https://github.com/jndok/tpwn-bis
https://github.com/wzw19890321/OSX_vul
https://github.com/linusyang/SSLPatch

公开的 IOS 越狱源码：
IOS6.1.3~6.1.6 的越狱源码
https://github.com/p0sixspwn/p0sixspwn
IOS8.4.1 的越狱源码
https://github.com/kpwn/yalu

OSX/IOS 漏洞主要集中在如下几个方面：
Bypass Something
CSRF
Denial Of Service
Directory Traversal
Execute Code
Gain Information
Gain Privilege
Memory Corruption
Overflow
SQL Injection
XSS
目前在 OSX/IOS 应用层主要发现的集中在 XSS,SQL Injection,CSRF,Gain Information,Denial Of Service 等漏洞,系统层主要集中在:Bypass Something,Denial Of Service,Gain Privilege,Overflow 等

今天抽时间整理了这些资料，主要是方便自己复习研究，要想多挖 OSX/IOS 系统漏洞，还是得多花时间，好好研读 OSX 系统源码，链接：http://opensource.apple.com/，还有就是多动手，多思考，多学习吧，这条路还蛮长的，要学的东西还有很多，上面仅仅是对自己之前学习的一个总结，古人说的好：学习要善于总结，温故而之新，有时候我们学习的一些知识很容易被忘记，这样就需要我们时不时拿出来研究，学习，这样才能达到一个更高的层次，好了，今天就给大家总结到这里，就作为我上一篇《IOS 安全学习笔记》的“兄弟”pdf 吧，这个 pdf 主要集中研究 OSX/IOS 漏洞以及越狱方面的知识，后面会定期更新一些知识点，希望能和更多在这方面感兴趣的人一起研究，路还很长，慢慢摸索吧！