表格 1

	CVE描述	苹果描述	影响	模块	版本	poc	poc状态
CVE-2014-9495	在1.5.21版本之前，以及1.6.x且1.6.16版本之前的libpng中的png_combine_row函数存在堆溢出，在64位操作系统中，允许攻击者通过构造的PNG图片执行任意代码	1.6.20版本前的libpng存在多个漏洞导致任意代码执行	任意代码执行	python	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	http://tfpwn.com/files/libpng_heap_overflow_1.6.15.txt	未验证
CVE-2015-0973	libpng 1.5.21之前版本和1.6.16之前1.6.x版本的pngrutil.c文件中的'png_read_IDAT_data'函数存在缓冲区溢出漏洞。攻击者可借助带有超长宽度的IDAT数据利用该漏洞执行任意代码。	1.6.20版本前的libpng存在多个漏洞导致任意代码执行	任意代码执行	python	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	http://tfpwn.com/files/libpng_heap_overflow_1.6.15.txt	未验证
CVE-2015-1819	libxml2是XML解析程序和标记工具集。 libxml2未正确处理某些XML数据。通过精心构造的文档，攻击者造成资源耗尽，导致拒绝服务。	通过一个而已的XML文件可能导致DOS或者任意代码执行	DOS	libxml2	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2015-3195	OpenSSL 0.9.8zh之前版本,1.0.0-1.0.0t, 1.0.1-1.0.1q, 1.0.2-1.0.2e版本crypto/asn1/tasn_dec.c中，ASN1_TFLG_COMBINE在实现上错误处理了畸形X509_ATTRIBUTE数据造成的错误。通过触发PKCS#7或CMS应用的解码失败，远程攻击者利用此漏洞可获取进程内存的敏感信息。	0.98zh之前的openssl存在一个内存泄露的问题将导致DOS	DOS	OpenSSL	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2015-5312	2.9.3之前的libxml在parser.c中的xmlStringLenDecodeEntities函数存在一个漏洞， libxml2未正确处理某些XML数据。通过精心构造的文档，攻击者造成资源耗尽，导致拒绝服务。	通过一个而已的XML文件可能导致DOS或者任意代码执行	DOS	libxml2	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2015-7499	在libxml2的实现中存在内存破坏安全漏洞，处理恶意构造的XML过程中可导致应用意外中止或任意代码执行	通过一个而已的XML文件可能导致DOS或者任意代码执行	DOS	libxml2	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2015-7500	libxml2 2.9.3之前版本，函数xmlParseMisc存在安全漏洞，上下文独立的攻击者利用此漏洞可造成拒绝服务（越界堆读）。	通过一个而已的XML文件可能导致DOS或者任意代码执行	DOS	libxml2	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2015-7551	Fiddle 與 DL 函式庫發現了不安全的字串用途瑕疵所產生的安全性風險。本問題初見於 DL 的 CVE-2009-5147，但在 DL 重新使用 Fiddle 和 libffi 實作後重新發現。 CVE-2009-5147 曾在 Ruby 1.9.1 版本修復，但其它分支並未修復，Ruby 1.9 系列除了 1.9.1 之外，有打包 DL 的版本都存在此安全性風險。	本地攻击者可能导致DOS或者任意代码执行	DOS 任意代码执行	Ruby	OS X El Capitan v10.11 to v10.11.3	https://www.ruby-lang.org/zh_tw/news/2015/12/16/unsafe-tainted-string-usage-in-fiddle-and-dl-cve-2015-7551/	未验证
CVE-2015-7942	libxml2是XML解析程序和标记工具集。 libxml2 停止解析某些无效的XML数据时，parser.c内的xmlParseConditionalSections函数未正确跳过中介实体。通过构造的XML数据，上下文攻击者造成资源耗尽，导致拒绝服务。	通过一个而已的XML文件可能导致DOS或者任意代码执行	DOS	libxml2	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	https://bugzilla.gnome.org/show_bug.cgi?id=744980#c7	未验证
CVE-2015-8035	libxml2的实现中存在内存破坏安全漏洞，处理恶意构造的XML过程中可导致应用意外中止或任意代码执行。	通过一个而已的XML文件可能导致DOS或者任意代码执行	DOS	libxml2	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	https://bugzilla.gnome.org/show_bug.cgi?id=757466	未验证
CVE-2015-8126	libpng是适用于多种应用程序的PNG图形解析函数库。 libpng某些版本的函数png_set_PLTE及png_get_PLTE存在多个缓冲区溢出漏洞，通过PNG图形IHDR块内较小的位深值，远程攻击者利用此漏洞可造成拒绝服务（应用崩溃）。	通过一个构造的png文件导致任意代码执行	任意代码执行	Tcl	OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	https://bugs.chromium.org/p/chromium/issues/detail?id=560291	未验证
CVE-2015-8242	libxml2是XML解析程序和标记工具集。 libxml2 2.9.3之前版本，函数xmlSAX2TextNode（HTML解析器push接口的SAX2.C内）存在安全漏洞，通过构造的XML数据，上下文独立的攻击者利用此漏洞可造成拒绝服务（栈缓冲区溢出及应用崩溃）或获取敏感信息。	通过一个而已的XML文件可能导致DOS或者任意代码执行	DOS	libxml2	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	https://bugzilla.gnome.org/show_bug.cgi?id=756372	未验证
CVE-2015-8472	libpng是适用于多种应用程序的PNG图形解析函数库。 libpng某些版本，png_set_PLTE函数存在缓冲区溢出漏洞，远程攻击者通过PNG图形中IHDR块内较小的位深值，利用此漏洞可造成拒绝服务（应用崩溃）。	1.6.20版本前的libpng存在多个漏洞导致任意代码执行	任意代码执行	Python apache_mod_php	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	未发现	未验证
CVE-2015-8659	HTTPProtocol的实现中，nghttp2 1.6.0之前版本存在安全漏洞，可导致远程执行任意代码。	HTTPProtocol的实现中，nghttp2 1.6.0之前版本存在安全漏洞，可导致远程执行任意代码。	远程任意代码执行	HTTPProtocol	OS X El Capitan v10.11 to v10.11.3	未发现	未验证
CVE-2016-0777	OpenSSH是SSH协议的开源实现。 OpenSSH 5.x, 6.x, 7.1p2之前的7.x版本，client内roaming_common.c的函数resend_bytes存在安全漏洞，远程攻击者通过请求传输整个缓冲区，利用此漏洞可获取进程内存的敏感信息。	连接到服务器有可能泄露用户信息，私钥	信息泄露	OpenSSH	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	https://www.qualys.com/2016/01/14/cve-2016-0777-cve-2016-0778/openssh-cve-2016-0777-cve-2016-0778.txt	未验证
CVE-2016-0778	OpenSSH是SSH协议的开源实现。 OpenSSH 5.x, 6.x, 7.1p2之前的7.x版本，启用了某些代理及转发选项后，roaming_common.c内的函数roaming_read及roaming_write未正确保留连接文件描述符，这可使远程服务器造成拒绝服务（堆缓冲区溢出）。	连接到服务器有可能泄露用户信息，私钥	DOS	OpenSSH	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	https://www.qualys.com/2016/01/14/cve-2016-0777-cve-2016-0778/openssh-cve-2016-0777-cve-2016-0778.txt	未验证
CVE-2016-0801 **CVE-2016-0802**	Android的kernel中的Broadcom Wi-Fi驱动程序中存在安全漏洞。远程攻击者可借助特制的无线控制消息数据包利用该漏洞造成拒绝服务（内存破坏）或执行任意代码。	有权限的攻击者可以执行任意代码	任意代码执行	Wi-Fi	Available for: OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1732	可以泄露内核的真实地址,从而为其他针对内核的攻击创造条件	可以泄露内核的真实地址,从而为其他针对内核的攻击创造条件	信息泄露	AppleRAID	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1733	通过非法的数据输入导致内存腐坏	可以造成内核代码执行	内核代码执行	AppleRAID	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1734	AppleUSBNetworking模块漏洞导致内核代码执行	usb驱动解析数据时会导致内存腐坏，导致内核权限代码执行	内核代码执行	AppleUSBNetworking	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1735	蓝牙模块漏洞导致任意代码执行，拒绝服务	在内存操作中存在多个内存腐坏，导致内核权限代码执行	内核代码执行	Bluetooth	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1736	蓝牙模块漏洞导致任意代码执行，拒绝服务	在内存操作中存在多个内存腐坏，导致内核权限代码执行	内核代码执行	Bluetooth	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1737	carbon模块 通过处理恶意的.dfont文件导致远程代码执行或者拒接服务	在处理字体文件的时候存在多处内存腐坏	任意代码执行	Carbon	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1738	dyld允许攻击者通过修改app跳过数字签名	数字签名模块中存在问题	绕过签名	dyld	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1740	通过恶意的PDF文件，FontParser模块导致攻击者任意执行代码或者拒绝服务	内存处理中存在内存腐坏问题	任意代码执行 DOS	FontParser	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1741	通过恶意的APP，NVIDIA驱动模块导致攻击者任意执行代码或者拒绝服务	内存处理中存在内存腐坏问题	任意代码执行 DOS	NVIDIA Graphics Drivers	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1743	通过恶意的APP，Inter驱动模块导致攻击者任意执行代码或者拒绝服务	内存处理中存在内存腐坏问题，可能拥有内核代码执行权限	内核代码执行	Intel Graphics Driver	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1744	通过恶意的APP，Inter驱动模块导致攻击者任意执行代码或者拒绝服务	内存处理中存在内存腐坏问题，可能拥有内核代码执行权限	内核代码执行	Intel Graphics Driver	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1745	通过vectors，IOFireWireFamily模块会导致拒绝服务，空指针	空指针引用导致DOS	DOS	IOFireWireFamily	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1746	通过恶意的APP， IOGraphics驱动模块导致攻击者任意执行代码或者拒绝服务	不合法的输入导致内存腐坏	内核权限代码执行	IOGraphics	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1747	通过恶意的APP， IOGraphics驱动模块导致攻击者任意执行代码或者拒绝服务	不合法的输入导致内存腐坏	内核权限代码执行	IOGraphics	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1748	通过恶意的APP， IOHIDFamily驱动模块导致攻击者获得内核的内存信息泄露	内存处理时导致内存的腐坏	信息泄露	IOHIDFamily	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1749	通过恶意的APP， IOUSBFamily驱动模块导致内核权限代码执行	内存处理时有多个会导致内存腐坏的问题	内核权限代码执行	IOUSBFamily	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1750	通过恶意的APP， 出发内核的UAF从而执行内核权限的代码	内场管理的模块存在UAF的漏洞	内核权限代码执行	Kernel	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1752	通过恶意的APP， 攻击者通过内核的漏洞造成拒绝服务	A denial of service issue was addressed through improved validation.	DOS	Kernel	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1753	内核存在整数溢出问题导致内核权限代码执行	存在多个因为不合法的输入导致的整数溢出	内核权限代码执行	Kernel	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1754 **CVE-2016-1755** **CVE-2016-1759**	通过恶意的APP导致内核拒绝服务以及内核权限代码执行	内存处理存在多个问题导致内存腐坏	内核代码执行 DOS	Kernel	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1756	内核存在空指针引用，导致任意代码执行以及拒绝服务	异常的输入导致空指针引用	任意代码执行	Kernel	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1757	通过恶意的APP，利用内核的条件竞争导致任意代码执行	创建新的进程时存在条件竞争的问题	任意代码执行	Kernel	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1758	通过恶意的APP，获取内核真是地址或者拒绝服务	异常的输入导致内存越界	信息泄露	Kernel	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1761 **CVE-2016-1762**	通过一个恶意的XML文件，攻击者利用libxml2的漏洞导致任意代码执行或者拒绝服务	通过一个而已的XML文件可能导致DOS或者任意代码执行	任意代码执行 DOS	libxml2	OS X Mavericks v10.9.5 OS X Yosemite v10.10.5 OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1764	通过javascript：URL，CSP模块获取敏感信息	javascript的连接处理存在一个漏洞	信息泄露	Messages	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1767 **CVE-2016-1768**	通过恶意的FlashPix文件可以导致任意代码执行或者拒绝服务	内存处理时存在多个问题导致内存腐坏	任意代码执行 DOS	QuickTime	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1769	通过恶意的Photoshop文件可以导致任意代码执行或者拒绝服务	内存处理时存在多个问题导致内存腐坏	任意代码执行 DOS	QuickTime	OS X El Capitan v10.11 to v10.11.3	未发现	

	CVE描述	苹果描述	影响	模块	版本	poc	poc状态
CVE-2016-1770	The Reminders component in Apple OS X before 10.11.4 allows attackers to bypass an intended user-confirmation requirement and trigger a dialing action via a tel: URL.	点击一个tel link可以绕过用户播出一个电话	其他	Reminders	OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1773	数字签名模块没有正确的确认文件的拥有权。	数字签名工具存在权限问题，导致用户可以确认任意文件是否存在	其他	Security	Available for: OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1775	通过一个恶意的字体文件，TrueTypeScaler模块导致远程任意代码执行或者拒绝服务	异常的输入导致内存腐坏	远程任意代码执行 DOS	TrueTypeScaler	Available for: OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1788	messages里面存在问题，导致攻击者远程读取消息附件	A cryptographic issue was addressed by rejecting duplicate messages on the client.	信息泄露	Messages	Available for: OS X El Capitan v10.11 to v10.11.3	未发现	
CVE-2016-1950	Mozilla Network Security Services (NSS) 存在堆溢出，导致远程任意代码执行，通过恶意的asn.1	ASN.1 decoder存在内存腐坏的问题	任意代码执行	Security	Available for: OS X El Capitan v10.11 to v10.11.3	未发现	