iOS Exploits

Created by HP (193 pt), last modified by Ben M. ATTLER yesterday at 4:10 PM

iOS Exploits Data

Name	Type	Access Granted	Born Date & iOS Version	Modification Date	Death Date	Found by	Description
Archon	technique	Remote Architecture Detection				(came with purchase)	
Dyonedo	macho-parsing	Codesign Defeat				JDW - GCHQ	
Earth/Eve		Remote Exploit				Purchased by NSA Shared with CIA Ported by GCHQ	
Elderpiggy		Sandbox Escape				Peppermint (NSA VR Contract) Implemented by GCHQ at JDW	
Ironic		Kernel ASLR Defeat			iOS 8	Public vulnerability researcher: Steffan Esser (i0nic)	
Nandao	Heap overflow corruption?	Kernel Exploit				GCHQ	
Juggernaut						Purchase- Baitshop	
Persistence	Execution via symbolic links	Reboot Persistence	June 2013, JDW XXXX	June 2014, JDW XXXX		CIA	By selecting specific executables on the system partition that are run with root privileges, a symbolic link can be created (on iOS 7.x) or an existing file can be overwritten(iOS 8.x) that will run our bootstrapper, giving use initial execution on every boot.
Redux	Sandbox misconfiguration	Close Access	June 2012, iOS 6	7/15, workaround for missing vpnagent in iOS 8 dev dmgs	11/17/14, iOS 8.1.1	GCHQ	**Sandbox Profiles:** **Available for**: iPhone 4S and later, iPod touch (5th generation) and later, iPad 2 and later **Impact:** A malicious application may be able to launch arbitrary binaries on a trusted device **Description:** A permissions issue existed with the debugging functionality for iOS that allowed the spawning of applications on trusted devices that were not being debugged. This was addressed by changes to debugserver's sandbox. **Publicly discovered by the Chinese Jailbreak team, Pangu** **CVE: 2014-4457**
Rhino	API misuse	Kernel ASLR Defeat	April 2013, iOS 7		June 2014, iOS 8 Beta 1	GCHQ	Reads KEXT info that reveals the KASLR values by calling the OSKextCopyLoadedKextInfo function.
Sal	Abnormal code path in the kernel	Codesign Defeat	DATE???, iOS 7	2/15, bugfix		FBI, ROU	Copies non-paged sized chunks so that the vm_map_copy_overwrite_unaligned() path is taken in the kernel. This abnormal code path results in pages of memory not being paged in, so the cs_tainted flag is never set on the pages in memory, causing no signature checks.
Saline	Buffer Overflow caused by deserialization parsing error in Foundation library	ROP execution	DATE???, iOS 8	2/15, Productized at TRICLOPS workshop		Purchase - Baitshop	Sending a crafted NSArchiver object to any process that calls NSArchive unarchive method will result in a buffer overflow, allowing for ROP.
Wintersky	Size Mismatch between user and kernel structures	Kernel ASLR Defeat	DATE???, iOS 8			NOCTURNALFEARS	WinterSky leaks the kernel address of the ipc_port struct of a user provided mach port.
Xiphos	Validation Issue	Kernel Exploit	March 2014, iOS 7		11/14, iOS 8.1.1	CIA	**Available for:** iPhone 4S and later, iPod Touch 5th gen and later, iPad 2 and Later. **Impact:** A malicious application may be able to execute arbitrary code with system privileges. **Description:** A validation issue existed in the handling of certain metadata fields of ***IOSharedDataQueue*** objects. **Publicly discovered by the Chinese Jailbreak team, Pangu.**

Exploits

		Release Date(s)	Access	Kernel Info Leak	Kernel Exploit	Sandbox Escape (browser)	Code Sign Defeat	Persistence (reboot)	Persistence (update)
iOS 4 (4.0 - 4.3.3)	**Remote**	6/21/2010 - 3/11/2011	SafferonSkies	<NR>	<NR>	??	EarlyKatana	overrides.plist	No (OTA <NR>)
	Local		SLIDE			<NR>			
iOS 5 (5.0 - 5.1.1)	**Remote**	10/12/2011 - 5/7/2012	SunsetSkies	<NR>	Corona (5.0.1)	??	EarlyKatana	overrides.plist	Yes (sys not touched)
	Local		SLIDE		<NR>	<NR>			
iOS 6 (6.x - 6.1.2)	**Remote**	9/19/2012 - 2/16/2013	Wby	Rhino	Cutlass	SandShrew	Katana (libamfi)	overrides.plist launchd.conf	block
	Local		Redux			<NR>			
iOS 6 (6.1.3 - 6.1.4)	**Remote**	3/19/2013 - 5/2/2013	Wby	Rhino	Scimitar	SandShrew	Dyonedo	dirhelper	block
	Local		Redux			<NR>			
iOS 7 (7.0 - 7.1.2)	**Remote**	9/18/2013 - 6/20/2014	Eve	<NR>	Xiphos	Piggy	Dyonedo	dirhelper	block
	Local		Redux			<NR>			
iOS 8 (8.0 & 8.0.2)	**Remote**	9/17/2014 - 9/25/2014	Earth	Ironic	Nandao	<NR>	Dyonedo	dirhelper	block
	Local		Saline						
iOS 8 (8.1 - 8.1.2)	**Remote**	10/10/2014 - 12/19/2014	Earth	Ironic	Nandao	<NR>	Dyonedo	dirhelper	block
	Local		Saline						
iOS 8 (8.1.3 - 8.2)	**Remote**	1/27/2015 - 3/9/2015	Earth	WinterSky	Nandao	<NR>	Dyonedo	mount NFS	block
	Local		Saline						
IOS 8.3	**Remote**	4/8/2015	Earth	WinterSky	Nandao	<NR>	Juggernaut	mount NFS	block
	Local		Saline						
iOS 8.4	**Remote**	6/30/2015	Earth	WinterSky	Nandao	<NR>	Juggernaut	mount NFS	block
	Local		Saline						

Key	
	New Exploit
	Major Update
	Minor Update
	Minimal Changes
<NR>	Not Required
??	Unknown

Old Tables (To be removed)

iOS 4 (4.0 - 4.3.3)		iOS 5 (5.0 - 5.1.1)		iOS 6 (6.x - 6.1.2)		iOS 6.1.3 - 6.1.4		iOS 7		iOS
	Remote	**Local**	**Remote**	**Local**	**Remote**	**Local**	**Remote**	**Local**	**Remote**	**Local**
Kernel Info Leak	<NR>	<NR>	<NR>	<NR>	rhino	rhino	rhino	rhino	<NR>	<NR>
Sandbox Escape (browser)	??	<NR>	??	<NR>	sandshrew	<NR>	sandshrew	<NR>	piggy	<NR>
Kernel	<NR>	<NR>	<NR>,	<NR>	cutlass	cutlass	scimitar	scimitar	xiphos	xiphos

Exploit			CORONA(5.0.1)							
Code Sign Defeat	EARLYKATANA	EARLYKATANA	EARLYKATANA	EARLYKATANA	katana (libamfi)	katana (libamfi)	dyonedo	dyonedo	dyonedo	dyonedo
Access	SAFFRONSKIES (4.3 only?)	SLIDE	SUNSETSKIES	SLIDE	wby	redux	wby	redux	eve	redux
Persistence (reboot)	overrides.plist	overrides.plist	overrides.plist	overrides.plist	overrides.plist / launchd.conf	overrides.plist / launchd.conf	dirhelper	dirhelper	dirhelper	dirhelper
Persistence (update)	NO (OTA <NR>)	NO (OTA <NR>)	YES(sys not touched)	YES(sys not touched)	block	block	block	block	block	block

	iOS 8 (8.0 & 8.0.2)		**iOS 8.1 - 8.1.2**		**iOS 8.1.3 - 8.2**		**IOS 8.3**		**iOS 8.4**	
Release Date(s)	***9/17/2014 - 9/25/2014***		***10/10/2014 - 12/19/2014***		***1/27/2015 - 3/9/2015***		***4/8/2015***		***6/30/2015***	
	Remote	**Local**	**Remote**	**Local**	**Remote**	**Local**	**Remote**	**Local**	**Remote**	**Local**
Kernel Info Leak	Ironic	Ironic	Ironic	Ironic	WinterSky	WinterSky	WinterSky	WinterSky	WinterSky	WinterSky
Sandbox Escape (browser)	<NR>	<NR>	<NR>	<NR>	<NR>	<NR>	<NR>	<NR>	<NR>	<NR>
Kernel Exploit	Nandao	Nandao	Nandao	Nandao	Nandao	Nandao	Nandao	Nandao	Nandao	Nandao
Code Sign Defeat	dyonedo	dyonedo	dyonedo	dyonedo	dyonedo	dyonedo	Juggernaut	Juggernaut	Juggernaut	Juggernaut
Access	Earth	Saline	Earth	Saline	Earth	Saline	Earth	Saline	Earth	Saline
Persistence (reboot)	dirhelper	dirhelper	dirhelper	dirhelper	dirhelper	dirhelper	Mount NFS	Mount NFS	Mount NFS	Mount NFS
Persistence (update)	block	block	block	block	block	block	block	block	block	block

XX = required, but not available.

<NR> = not required

?? - Unknown / some else fill this in

No labels