Brian Beckerle

evasiOn

What is evasiOn?

Latest iPhone jailbreak, iOS 6.1

Patched in latest version iOS 6.1.3
4 of 6? Exploits fixed

"most elaborate jailbreak to ever hack your phone"
-forbes

Used 800,000 times in 6 hours after its release

Breaking out of iOS Jail

- iOS prevents
  - Installing or booting into a modified/different OS
  - Running unsigned apps
    - Main reason for jailbreaking (Cydia)
  - Apps from running outside a secure sandbox
    - Apps can't use root permissions, do anything outside assigned entitlements
- Jailbreaking allows you to do all these
  - Privilege escalation, also need to bypass other security

What's stopping us?

- iOS has evolved into a secure modern operating system
  - ASLR
  - Code-signing
  - DEP
  - Sandboxing/Privilege Separation
  - Made even more difficult by reduced attack surface
    - Stripped down version of OS X
    - No Java, Flash
    - Some file types rejected by Mobile Safari

First Roadblock

- How do we get the files onto the phone?
  - iOS restricts where users can place files
- MobileBackup
  - Daemon that creates and restores backups
  - Created by device and interchangeable between devices = not easily signed
  - Normally has path restrictions
  - Luckily a bug in backup allows symlinks between filepaths

The App

- Inserted in var/mobile using symlink trick
- Shell script
  - *#!/bin/launchctl submit -l remount -o /var/mobile/Media/mount.stdout -e /var/mobile/Media/mount.stderr -- /sbin/mount -v -t hfs -o rw /dev/disk0s1s1*
- Environment Variable
  - *LAUNCHD_SOCKET = /private/var/tmp/launchd/sock*

Getting Permission

- Bug in lockdownd
  - Lockdownd provides system info to clients
  - *root* privileges
  - Bug: change permissions of var/db/timezone to be accessible to *mobile*
- New backup is created
  - Symlink between var/db/timezone and var/tmp/launchd
  - Permissions granted by sending malformed request
  - Var/db/timezone and therefore var/tmp/launchd are now accessible by all users
  - Same trick repeated for subfolders:
    - var/tmp/launchd/sock

Running the App

- Launchd : daemon that deals with launching and shutting down processes
- Multiple instances, some have root permission
- Talk to them through sockets
  - Which socket you use determines which launchd you are talking to
  - The socket we got access to talks to the root launchd
  - Launches processes with root privileges

Making it stick

- System partition is now writable
- Make another backup
  - Launchd configuration file
  - Dynamic library that overrides MISValidate signature method to always return 0
  - An executable

The files

- launchd.conf

- *bsexec .. /sbin/mount -u -o rw,suid,dev*
- *setenv DYLD_INSERT_LIBRARIES /private/var/evasion/amfi.dylib*
- *load /System/Library/LaunchDaemons/*
  com.apple.MobileFileIntegrity.plist
- *bsexec .. /private/var/evasion/evasion*
- *unsetenv DYLD_INSERT_LIBRARIES*
- *bsexec .. /bin/rm -f /private/var/evasion/sock*
- *bsexec .. /bin/ln -f /var/tmp/launchd/sock /private/var/evasion/sock*

The files

- amfi.dylib

  $ dyldinfo –export amfi.dylib

  export information (from trie):

  [re-export] _kMISValidationOptionValidateSignatureOnly (_kCFUserNotificationTokenKey from CoreFoundation)

  [re-export] _kMISValidationOptionExpectedHash (_kCFUserNotificationTimeoutKey from CoreFoundation)

  [re-export] _MISValidateSignature (_CFEqual from CoreFoundation)

Sources

- http://blog.accuvantlabs.com/blog/bthomas/evasion-jailbreaks-userland-component
- http://www.forbes.com/sites/andygreenberg/2013/02/05/inside-evasion-the-most-elaborate-jailbreak-to-ever-hack-your-iphone/#
- iOS hacker's handbook – Charlie Miller, Dionysus Blazakis
- http://en.wikipedia.org/wiki/IOS_jailbreaking
- http://developer.apple.com/library/ios/

Sources

- http://evasion.com/
- http://lists.apple.com/archives/security-announce/2013/Mar/msg00004.html

Bugs

dyld
Available for: iPhone 3GS and later,
iPod touch (4th generation) and later, iPad 2 and later
Impact: A local user may be able to execute unsigned code
Description: A state management issue existed in the handling of Mach-O executable files with overlapping segments. This issue was addressed by refusing to load an executable with overlapping segments.
CVE-ID
CVE-2013-0977 : evad3rs

Kernel
Available for: iPhone 3GS and later,
iPod touch (4th generation) and later, iPad 2 and later
Impact: A local user may be able to determine the address of structures in the kernel
Description: An information disclosure issue existed in the ARM prefetch abort handler. This issue was addressed by panicking if the prefetch abort handler is not being called from an abort context.
CVE-ID
CVE-2013-0978 : evad3rs

USB
Available for: iPhone 3GS and later,
iPod touch (4th generation) and later, iPad 2 and later
Impact: A local user may be able to execute arbitrary code in the kernel
Description: The IOUSBDeviceFamily driver used pipe object pointers that came from userspace. This issue was addressed by performing additional validation of pipe object pointers.
CVE-ID
CVE-2013-0981 : evad3rs

Lockdown
Available for: iPhone 3GS and later,
iPod touch (4th generation) and later, iPad 2 and later
Impact: A local user may be able to change permissions on arbitrary files
Description: When restoring from backup, lockdownd changed permissions on certain files even if the path to the file included a symbolic link. This issue was addressed by not changing permissions on any file with a symlink in its path.
CVE-ID
CVE-2013-0979 : evad3rs