About the security content of iOS 7

This document describes the security content of iOS 7.

For the protection of our customers, Apple does not disclose, discuss, or confirm security issues until a full investigation has occurred and any necessary patches or releases are available. To learn more about Apple Product Security, see the Apple Product Security website.

For information about the Apple Product Security PGP Key, see How to use the Apple Product Security PGP Key.

Where possible, CVE IDs are used to reference the vulnerabilities for further information.

To learn about other Security Updates, see Apple Security Updates.

iOS 7

- **Certificate Trust Policy**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Root certificates have been updated

  Description: Several certificates were added to or removed from the list of system roots.

- **CoreGraphics**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Viewing a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution

  Description: A buffer overflow existed in the handling of JBIG2 encoded data in PDF files. This issue was addressed through additional bounds checking.

  CVE-ID

  CVE-2013-1025 : Felix Groebert of the Google Security Team

- **CoreMedia**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Playing a maliciously crafted movie file may lead to an unexpected application termination or arbitrary code execution

  Description: A buffer overflow existed in the handling of Sorenson encoded movie files. This issue was addressed through improved bounds checking.

  CVE-ID

  CVE-2013-1019 : Tom Gallagher (Microsoft) & Paul Bates (Microsoft) working with HP's Zero Day Initiative

- **Data Protection**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Apps could bypass passcode-attempt restrictions

  Description: A privilege separation issue existed in Data Protection. An app within the third-party sandbox could repeatedly attempt to determine the user's passcode regardless of the user's "Erase Data" setting. This issue was addressed by requiring additional entitlement checks.

  CVE-ID

CVE-2013-0957 : Jin Han of the Institute for Infocomm Research working with Qiang Yan and Su Mon Kywe of Singapore Management University

- **Data Security**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: An attacker with a privileged network position may intercept user credentials or other sensitive information

  Description: TrustWave, a trusted root CA, has issued, and subsequently revoked, a sub-CA certificate from one of its trusted anchors. This sub-CA facilitated the interception of communications secured by Transport Layer Security (TLS). This update added the involved sub-CA certificate to OS X's list of untrusted certificates.

  CVE-ID

  CVE-2013-5134

- **dyld**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: An attacker who has arbitrary code execution on a device may be able to persist code execution across reboots

  Description: Multiple buffer overflows existed in dyld's openSharedCacheFile() function. These issues were addressed through improved bounds checking.

  CVE-ID

  CVE-2013-3950 : Stefan Esser

- **File Systems**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: An attacker who can mount a non-HFS filesystem may be able to cause an unexpected system termination or arbitrary code execution with kernel privileges

  Description: A memory corruption issue existed in the handling of AppleDouble files. This issue was addressed by removing support for AppleDouble files.

  CVE-ID

  CVE-2013-3955 : Stefan Esser

- **ImageIO**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Viewing a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution

  Description: A buffer overflow existed in the handling of JPEG2000 encoded data in PDF files. This issue was addressed through additional bounds checking.

  CVE-ID

  CVE-2013-1026 : Felix Groebert of the Google Security Team

- **IOKit**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Background applications could inject user interface events into the foreground app

  Description: It was possible for background applications to inject user interface events into the foreground application using the task completion or VoIP APIs. This issue was addressed by enforcing access controls on foreground and background processes that handle interface events.

  CVE-ID

CVE-2013-5137 : Mackenzie Straight at Mobile Labs

- **IOKitUser**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: A malicious local application could cause an unexpected system termination

  Description: A null pointer dereference existed in IOCatalogue. The issue was addressed through additional type checking.

  CVE-ID

  CVE-2013-5138 : Will Estes

- **IOSerialFamily**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Executing a malicious application may result in arbitrary code execution within the kernel

  Description: An out of bounds array access existed in the IOSerialFamily driver. This issue was addressed through additional bounds checking.

  CVE-ID

  CVE-2013-5139 : @dent1zt

- **IPSec**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: An attacker may intercept data protected with IPSec Hybrid Auth

  Description: The DNS name of an IPSec Hybrid Auth server was not being matched against the certificate, allowing an attacker with a certificate for any server to impersonate any other. This issue was addressed by improved certificate checking.

  CVE-ID

  CVE-2013-1028 : Alexander Traud of www.traud.de

- **Kernel**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: A remote attacker can cause a device to unexpectedly restart

  Description: Sending an invalid packet fragment to a device can cause a kernel assert to trigger, leading to a device restart. The issue was addressed through additional validation of packet fragments.

  CVE-ID

  CVE-2013-5140 : Joonas Kuorilehto of Codenomicon, an anonymous researcher working with CERT-FI, Antti LevomÃ¤ki and Lauri Virtanen of Vulnerability Analysis Group, Stonesoft

- **Kernel**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: A malicious local application could cause device hang

  Description: An integer truncation vulnerability in the kernel socket interface could be leveraged to force the CPU into an infinite loop. The issue was addressed by using a larger sized variable.

  CVE-ID

  CVE-2013-5141 : CESG

- **Kernel**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: An attacker on a local network can cause a denial of service

Description: An attacker on a local network can send specially crafted IPv6 ICMP packets and cause high CPU load. The issue was addressed by rate limiting ICMP packets before verifying their checksum.

CVE-ID

CVE-2011-2391 : Marc Heuse

- **Kernel**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Kernel stack memory may be disclosed to local users

  Description: An information disclosure issue existed in the msgctl and segctl APIs. This issue was addressed by initializing data structures returned from the kernel.

  CVE-ID

  CVE-2013-5142 : Kenzley Alphonse of Kenx Technology, Inc

- **Kernel**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Unprivileged processes could get access to the contents of kernel memory which could lead to privilege escalation

  Description: An information disclosure issue existed in the mach_port_space_info API. This issue was addressed by initializing the iin_collision field in structures returned from the kernel.

  CVE-ID

  CVE-2013-3953 : Stefan Esser

- **Kernel**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Unprivileged processes may be able to cause an unexpected system termination or arbitrary code execution in the kernel

  Description: A memory corruption issue existed in the handling of arguments to the posix_spawn API. This issue was addressed through additional bounds checking.

  CVE-ID

  CVE-2013-3954 : Stefan Esser

- **Kext Management**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: An unauthorized process may modify the set of loaded kernel extensions

  Description: An issue existed in kextd's handling of IPC messages from unauthenticated senders. This issue was addressed by adding additional authorization checks.

  CVE-ID

  CVE-2013-5145 : "Rainbow PRISM"

- **libxml**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Viewing a maliciously crafted web page may lead to an unexpected application termination or arbitrary code execution

  Description: Multiple memory corruption issues existed in libxml. These issues were addressed by updating libxml to version 2.9.0.

  CVE-ID

CVE-2011-3102 : Jüri Aedla

CVE-2012-0841

CVE-2012-2807 : Jüri Aedla

CVE-2012-5134 : Google Chrome Security Team (Jüri Aedla)

- **libxslt**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Viewing a maliciously crafted web page may lead to an unexpected application termination or arbitrary code execution

  Description: Multiple memory corruption issues existed in libxslt. These issues were addressed by updating libxslt to version 1.1.28.

  CVE-ID

  CVE-2012-2825 : Nicolas Gregoire

  CVE-2012-2870 : Nicolas Gregoire

  CVE-2012-2871 : Kai Lu of Fortinet's FortiGuard Labs, Nicolas Gregoire

- **Passcode Lock**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: A person with physical access to the device may be able to bypass the screen lock

  Description: A race condition issue existed in the handling of phone calls and SIM card ejection at the lock screen. This issue was addressed through improved lock state management.

  CVE-ID

  CVE-2013-5147 : videosdebarraquito

- **Personal Hotspot**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: An attacker may be able to join a Personal Hotspot network

  Description: An issue existed in the generation of Personal Hotspot passwords, resulting in passwords that could be predicted by an attacker to join a user's Personal Hotspot. The issue was addressed by generating passwords with higher entropy.

  CVE-ID

  CVE-2013-4616 : Andreas Kurtz of NESO Security Labs and Daniel Metz of University Erlangen-Nuremberg

- **Push Notifications**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: The push notification token may be disclosed to an app contrary to the user's decision

  Description: An information disclosure issue existed in push notification registration. Apps requesting access to the push notification access received the token before the user approved the app's use of push notifications. This issue was addressed by withholding access to the token until the user has approved access.

  CVE-ID

  CVE-2013-5149 : Jack Flintermann of Grouper, Inc.

- **Safari**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

Impact: Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution

Description: A memory corruption issue existed in the handling of XML files. This issue was addressed through additional bounds checking.

CVE-ID

CVE-2013-1036 : Kai Lu of Fortinet's FortiGuard Labs

- **Safari**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: History of pages recently visited in an open tab may remain after clearing of history

  Description: Clearing Safari's history did not clear the back/forward history for open tabs. This issue was addressed by clearing the back/forward history.

  CVE-ID

  CVE-2013-5150

- **Safari**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Viewing files on a website may lead to script execution even when the server sends a 'Content-Type: text/plain' header

  Description: Mobile Safari sometimes treated files as HTML files even when the server sent a 'Content-Type: text/plain' header. This may lead to cross-site scripting on sites that allow users to upload files. This issue was addressed through improved handling of files when 'Content-Type: text/plain' is set.

  CVE-ID

  CVE-2013-5151 : Ben Toews of Github

- **Safari**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Visiting a malicious website may allow an arbitrary URL to be displayed

  Description: A URL bar spoofing issue existed in Mobile Safari. This issue was addressed through improved URL tracking.

  CVE-ID

  CVE-2013-5152 : Keita Haga of keitahaga.com, Łukasz Pilorz of RBS

- **Sandbox**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Applications that are scripts were not sandboxed

  Description: Third-party applications which used the #! syntax to run a script were sandboxed based on the identity of the script interpreter, not the script. The interpreter may not have a sandbox defined, leading to the application being run unsandboxed. This issue was addressed by creating the sandbox based on the identity of the script.

  CVE-ID

  CVE-2013-5154 : evad3rs

- **Sandbox**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Applications can cause a system hang

Description: Malicious third-party applications that wrote specific values to the /dev/random device could force the CPU to enter an infinite loop. This issue was addressed by preventing third-party applications from writing to /dev/random.

CVE-ID

CVE-2013-5155 : CESG

- **Social**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Users recent Twitter activity could be disclosed on devices with no passcode.

  Description: An issue existed where it was possible to determine what Twitter accounts a user had recently interacted with. This issue was resolved by restricting access to the Twitter icon cache.

  CVE-ID

  CVE-2013-5158 : Jonathan Zdziarski

- **Springboard**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: A person with physical access to a device in Lost Mode may be able to view notifications

  Description: An issue existed in the handling of notifications when a device is in Lost Mode. This update addresses the issue with improved lock state management.

  CVE-ID

  CVE-2013-5153 : Daniel Stangroom

- **Telephony**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Malicious apps could interfere with or control telephony functionality

  Description: An access control issue existed in the telephony subsystem. Bypassing supported APIs, sandboxed apps could make requests directly to a system daemon interfering with or controlling telephony functionality. This issue was addressed by enforcing access controls on interfaces exposed by the telephony daemon.

  CVE-ID

  CVE-2013-5156 : Jin Han of the Institute for Infocomm Research working with Qiang Yan and Su Mon Kywe of Singapore Management University; Tielei Wang, Kangjie Lu, Long Lu, Simon Chung, and Wenke Lee from the Georgia Institute of Technology

- **Twitter**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Sandboxed apps could send tweets without user interaction or permission

  Description: An access control issue existed in the Twitter subsystem. Bypassing supported APIs, sandboxed apps could make requests directly to a system daemon interfering with or controlling Twitter functionality. This issue was addressed by enforcing access controls on interfaces exposed by the Twitter daemon.

  CVE-ID

  CVE-2013-5157 : Jin Han of the Institute for Infocomm Research working with Qiang Yan and Su Mon Kywe of Singapore Management University; Tielei Wang, Kangjie Lu, Long Lu, Simon Chung, and Wenke Lee from the Georgia Institute of Technology

- **WebKit**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

Impact: Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution

Description: Multiple memory corruption issues existed in WebKit. These issues were addressed through improved memory handling.

CVE-ID

CVE-2013-0879 : Atte Kettunen of OUSPG

CVE-2013-0991 : Jay Civelli of the Chromium development community

CVE-2013-0992 : Google Chrome Security Team (Martin Barbella)

CVE-2013-0993 : Google Chrome Security Team (Inferno)

CVE-2013-0994 : David German of Google

CVE-2013-0995 : Google Chrome Security Team (Inferno)

CVE-2013-0996 : Google Chrome Security Team (Inferno)

CVE-2013-0997 : Vitaliy Toropov working with HP's Zero Day Initiative

CVE-2013-0998 : pa_kt working with HP's Zero Day Initiative

CVE-2013-0999 : pa_kt working with HP's Zero Day Initiative

CVE-2013-1000 : Fermin J. Serna of the Google Security Team

CVE-2013-1001 : Ryan Humenick

CVE-2013-1002 : Sergey Glazunov

CVE-2013-1003 : Google Chrome Security Team (Inferno)

CVE-2013-1004 : Google Chrome Security Team (Martin Barbella)

CVE-2013-1005 : Google Chrome Security Team (Martin Barbella)

CVE-2013-1006 : Google Chrome Security Team (Martin Barbella)

CVE-2013-1007 : Google Chrome Security Team (Inferno)

CVE-2013-1008 : Sergey Glazunov

CVE-2013-1010 : miaubiz

CVE-2013-1037 : Google Chrome Security Team

CVE-2013-1038 : Google Chrome Security Team

CVE-2013-1039 : own-hero Research working with iDefense VCP

CVE-2013-1040 : Google Chrome Security Team

CVE-2013-1041 : Google Chrome Security Team

CVE-2013-1042 : Google Chrome Security Team

CVE-2013-1043 : Google Chrome Security Team

CVE-2013-1044 : Apple

CVE-2013-1045 : Google Chrome Security Team

CVE-2013-1046 : Google Chrome Security Team

CVE-2013-1047 : miaubiz

CVE-2013-2842 : Cyril Cattiaux

CVE-2013-5125 : Google Chrome Security Team

CVE-2013-5126 : Apple

CVE-2013-5127 : Google Chrome Security Team

CVE-2013-5128 : Apple

- **WebKit**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Visiting a malicious website may lead to information disclosure

  Description: An information disclosure issue existed in the handling of the window.webkitRequestAnimationFrame() API. A maliciously crafted website could use an iframe to determine if another site used window.webkitRequestAnimationFrame(). This issue was addressed through improved handling of window.webkitRequestAnimationFrame().

  CVE-ID
  CVE-2013-5159

- **WebKit**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Copying and pasting a malicious HTML snippet may lead to a cross-site scripting attack

  Description: A cross-site scripting issue existed in the handling of copied and pasted data in HTML documents. This issue was addressed through additional validation of pasted content.

  CVE-ID

  CVE-2013-0926 : Aditya Gupta, Subho Halder, and Dev Kar of xys3c (xysec.com)

- **WebKit**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Visiting a maliciously crafted website may lead to a cross-site scripting attack

  Description: A cross-site scripting issue existed in the handling of iframes. This issue was addressed through improved origin tracking.

  CVE-ID

  CVE-2013-1012 : Subodh Iyengar and Erling Ellingsen of Facebook

- **WebKit**

  Available for: iPhone 3GS and later, iPod touch (4th generation) and later, iPad 2 and later

  Impact: Visiting a maliciously crafted website may lead to an information disclosure

  Description: An information disclosure issue existed in XSSAuditor. This issue was addressed through improved handling of URLs.

  CVE-ID

  CVE-2013-2848 : Egor Homakov

- **WebKit**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Dragging or pasting a selection may lead to a cross-site scripting attack

  Description: Dragging or pasting a selection from one site to another may allow scripts contained in the selection to be executed in the context of the new site. This issue is addressed through additional validation of content before a paste or a drag and drop operation.

  CVE-ID

  CVE-2013-5129 : Mario Heiderich

- **WebKit**

  Available for: iPhone 4 and later, iPod touch (5th generation) and later, iPad 2 and later

  Impact: Visiting a maliciously crafted website may lead to a cross-site scripting attack

Description: A cross-site scripting issue existed in the handling of URLs. This issue was addressed through improved origin tracking.

CVE-ID

CVE-2013-5131 : Erling A Ellingsen

Published Date: 24 February 2017