About the security content of OS X Mavericks v10.9

This document describes the security content of OS X Mavericks v10.9.

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.

OS X Mavericks v10.9

- **Application Firewall**

  Impact: socketfilterfw --blockApp may not block applications from receiving network connections

  Description: The socketfilterfw command line tool's --blockApp option did not properly block applications from receiving network connections. This issue was addressed through improved handling of the --blockApp options.

  CVE-ID

  CVE-2013-5165 : Alexander Frangis of PopCap Games

- **App Sandbox**

  Impact: The App Sandbox may be bypassed

  Description: The LaunchServices interface for launching an application allowed sandboxed apps to specify the list of arguments passed to the new process. A compromised sandboxed application could abuse this to bypass the sandbox. This issue was addressed by disallowing sandboxed applications from specifying arguments.

  CVE-ID

  CVE-2013-5179 : Friedrich Graeter of The Soulmen GbR

- **Bluetooth**

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

  Description: The Bluetooth USB host controller deleted interfaces needed for later operations. This issue was addressed by retaining the interface until it is no longer needed.

  CVE-ID

  CVE-2013-5166 : Stefano Bianchi Mazzone, Mattia Pagnozzi, and Aristide Fattori of Computer and Network Security Lab (LaSER), Università degli Studi di Milano

- **CFNetwork**

  Impact: Session cookies may persist even after resetting Safari

  Description: Resetting Safari did not always delete session cookies until Safari was closed. This issue was addressed through improved handling of session cookies.

  CVE-ID

  CVE-2013-5167 : Graham Bennett, Rob Ansaldo of Amherst College

- **CFNetwork SSL**

  Impact: An attacker could decrypt part of a SSL connection

  Description: Only the SSLv3 and TLS 1.0 versions of SSL were used. These versions are subject to a protocol weakness when using block ciphers. A man-in-the-middle attacker could have injected invalid data, causing the

connection to close but revealing some information about the previous data. If the same connection was attempted repeatedly the attacker may eventually have been able to decrypt the data being sent, such as a password. This issue was addressed by enabling TLS 1.2.

CVE-ID

CVE-2011-3389

- **Console**

  Impact: Clicking on a malicious log entry may lead to unexpected application execution

  Description: This update modified the behavior of Console when clicking on a log entry with an attached URL. Rather than opening the URL, Console will now preview the URL with Quick Look.

  CVE-ID

  CVE-2013-5168 : Aaron Sigel of vtty.com

- **CoreGraphics**

  Impact: Windows may be visible over the lock screen after display sleep

  Description: A logic issue existed in CoreGraphics's handling of display sleep mode, resulting in data corruption that could result in windows being visible over the lock screen. The issue is addressed through improved handling of display sleep.

  CVE-ID

  CVE-2013-5169

- **CoreGraphics**

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

  Description: A buffer underflow existed in the handling of PDF files. This issue was addressed through improved bounds checking.

  CVE-ID

  CVE-2013-5170 : Will Dormann of the CERT/CC

- **CoreGraphics**

  Impact: An unprivileged application may be able to log keystrokes entered into other applications even when secure input mode is enabled

  Description: By registering for a hotkey event, an unprivileged application could log keystrokes entered into other applications even when secure input mode was enabled. This issue was addressed by additional validation of hotkey events.

  CVE-ID

  CVE-2013-5171

- **curl**

  Impact: Multiple vulnerabilities in curl

  Description: Multiple vulnerabilities existed in curl, the most serious of which may lead to arbitrary code execution. These issues were addressed by updating curl to version 7.30.0

  CVE-ID

  CVE-2013-0249

  CVE-2013-1944

- **dyld**

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

- **IOKitUser**

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

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

  CVE-ID

  CVE-2013-5138 : Will Estes

- **IOSerialFamily**

  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 improved bounds checking.

  CVE-ID

  CVE-2013-5139 : @dent1zt

- **Kernel**

  Impact: Use of SHA-2 digest functions in the kernel may result in an unexpected system termination

  Description: An incorrect output length was used for the SHA-2 family of digest functions, resulting in a kernel panic when these functions were used, primarily during IPSec connections. The issue was addressed through use of the expected output length.

  CVE-ID

  CVE-2013-5172 : Christoph Nadig of Lobotomo Software

- **Kernel**

  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**

  Impact: A local user may cause a denial of service

  Description: The kernel random number generator would hold a lock while satisfying a request from userspace, allowing a local user to make a large request and hold the lock for long periods of time, denying service to other users of the random number generator. This issue was addressed by releasing and reacquiring the lock for large requests more frequently.

  CVE-ID

  CVE-2013-5173 : Jaakko Pero of Aalto University

- **Kernel**

  Impact: A local, unprivileged user may be able to cause an unexpected system termination

Description: An integer sign issue existed in the handling of tty reads. This issue was addressed through improved handling of tty reads.

CVE-ID

CVE-2013-5174 : CESG

- **Kernel**

  Impact: A local user may be able to cause kernel memory information disclosure or an unexpected system termination

  Description: An out of bounds read issue existed in the handling of Mach-O files. This issue was addressed through improved bounds checking.

  CVE-ID

  CVE-2013-5175

- **Kernel**

  Impact: A local user may be able to cause a system hang

  Description: An integer truncation issue existed in the handling of tty devices. This issue was addressed through improved bounds checking.

  CVE-ID

  CVE-2013-5176 : CESG

- **Kernel**

  Impact: A local user may be able to cause an unexpected system termination

  Description: The kernel would panic when an invalid user-supplied iovec structure was detected. This issue was addressed through improved validation of iovec structures.

  CVE-ID

  CVE-2013-5177 : CESG

- **Kernel**

  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 improved bounds checking.

  CVE-ID

  CVE-2013-3954 : Stefan Esser

- **Kernel**

  Impact: Source specific multicast program may cause an unexpected system termination when using Wi-Fi network

  Description: An error checking issue existed in the handling of a multicast packets. This issue was addressed through improved handling of multicast packets.

  CVE-ID

  CVE-2013-5184 : Octoshape

- **Kernel**

  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**

  Impact: A malicious local application could cause a system hang

  Description: An integer truncation issue existed in the kernel socket interface, which 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

- **Kext Management**

  Impact: An unauthorized process can disable some loaded kernel extensions

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

  CVE-ID

  CVE-2013-5145 : "Rainbow PRISM"

- **LaunchServices**

  Impact: A file could show the wrong extension.

  Description: An issue exited in the handling of certain unicode characters that could allow filenames to show incorrect extensions. The issue was addressed by filtering unsafe unicode characters from display in filenames.

  CVE-ID

  CVE-2013-5178 : Jesse Ruderman of Mozilla Corporation, Stephane Sudre of Intego

- **Libc**

  Impact: Under unusual circumstances some random numbers may be predictable

  Description: If the kernel random number generator was not accessible to srandomdev(), the function fell back to an alternative method which had been removed by optimization, leading to a lack of randomness. This issue was addressed by modifying the code to be correct under optimization.

  CVE-ID

  CVE-2013-5180 : Xi Wang

- **Mail Accounts**

  Impact: Mail may not choose the most secure authentication method available

  Description: When auto-configuring a mail account on certain mailservers, the Mail app would choose plaintext authentication over CRAM-MD5 authentication. This issue was addressed through improved logic handling.

  CVE-ID

  CVE-2013-5181

- **Mail Header Display**

  Impact: An unsigned message may appear to be validly signed.

  Description: A logic issue existed in Mail's handling of unsigned messages that nevertheless contained a `multipart/signed` part. The issue was addressed through improved handling of unsigned messages.

  CVE-ID

  CVE-2013-5182 : Michael Roitzsch of Technische Universität Dresden

- **Mail Networking**

Impact: Information may be briefly transferred in plain text when non-TLS encryption is configured.

Description: When Kerberos authentication was enabled and Transport Layer Security was disabled, Mail would send some unencrypted data to the mail server, leading to an unexpected termination of the connection. The issue was addressed through improved handling of this configuration.

CVE-ID

CVE-2013-5183 : Richard E. Silverman of www.qoxp.net

- **OpenLDAP**

  Impact: The ldapsearch command line tool did not honor the minssf configuration

  Description: The ldapsearch command line tool did not honor the minssf configuration, which could lead to weak encryption being allowed unexpectedly. This issue was addressed through improved handling of the minssf configuration.

  CVE-ID

  CVE-2013-5185

- **perl**

  Impact: Perl scripts may be vulnerable to denial of service.

  Description: The rehash mechanism in outdated versions of Perl may be vulnerable to denial of service in scripts that use untrusted input as hash keys. The issue is addressed by updating to Perl 5.16.2.

  CVE-ID

  CVE-2013-1667

- **Power Management**

  Impact: The screen lock may not engage after the specified time period

  Description: A locking issue existed in power assertion management. The issue was addressed through improved lock handling.

  CVE-ID

  CVE-2013-5186 : David Herman at Sensible DB Design

- **python**

  Impact: Multiple vulnerabilities in python 2.7

  Description: Multiple vulnerabilities existed in python 2.7.2, the most serious of which may lead to decryption of the content of a SSL connection. This update addresses the issues by updating python to version 2.7.5. Further information is available via the python site at http://www.python.org/download/releases/

  CVE-ID

  CVE-2011-3389

  CVE-2011-4944

  CVE-2012-0845

  CVE-2012-0876

  CVE-2012-1150

- **python**

  Impact: Multiple vulnerabilities in python 2.6

  Description: Multiple vulnerabilities existed in python 2.6.7, the most serious of which may lead to decryption of the content of a SSL connection. This update addresses the issues by updating python to version 2.6.8 and applying the patch for CVE-2011-4944 from the Python project. Further information is available via the python site at

http://www.python.org/download/releases/

CVE-ID

CVE-2011-3389

CVE-2011-4944

CVE-2012-0845

CVE-2012-0876

CVE-2012-1150

- **ruby**

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

  Description: A hostname validation issue existed in Ruby's handling of SSL certificates. This issue was addressed by updating Ruby to version 2.0.0p247.

  CVE-ID

  CVE-2013-4073

- **Security**

  Impact: Support for X.509 certificates with MD5 hashes may expose users to spoofing and information disclosure as attacks improve

  Description: Certificates signed using the MD5 hash algorithm were accepted by OS X. This algorithm has known cryptographic weaknesses. Further research or a misconfigured certificate authority could have allowed the creation of X.509 certificates with attacker controlled values that would have been trusted by the system. This would have exposed X.509 based protocols to spoofing, man in the middle attacks, and information disclosure. This update disables support for an X.509 certificate with an MD5 hash for any use other than as a trusted root certificate.

  CVE-ID

  CVE-2011-3427

- **Security - Authorization**

  Impact: An administrator's security preferences may not be respected

  Description: The "Require an administrator password to access system preferences with lock icons" setting allows administrators to add an additional layer of protection to sensitive system settings. In some cases where an administrator had enabled this setting, applying a software update or upgrade could have subsequently disabled the setting. This issue was addressed through improved handling of authorization rights.

  CVE-ID

  CVE-2013-5189 : Greg Onufer

- **Security - Smart Card Services**

  Impact: Smart Card Services may be unavailable when certificate revocation checks are enabled

  Description: "A logic issue existed in OS X's handling of Smart Card certificate revocation checks. The issue was addressed through improved certificate revocation support.

  CVE-ID

  CVE-2013-5190 : Yongjun Jeon of Centrify Corporation

- **Screen Lock**

  Impact: The "Lock Screen" command may not take effect immediately

  Description: The "Lock Screen" command in the Keychain Status menu bar item did not take effect until after the "Require password [amount of time] after sleep or screen saver begins" setting had elapsed.

CVE-ID

CVE-2013-5187 : Michael Kisor of OrganicOrb.com, Christian Knappskog of NTNU (Norwegian University of Science and Technology), Stefan Grönke (CCC Trier), Patrick Reed

- **Screen Lock**

  Impact: A hibernated Mac with Autologin may not require a password to wake

  Description: A Mac with hibernation and autologin enabled may allow waking from hibernation without prompting for a password. This issue was addressed through improved lock handling.

  CVE-ID

  CVE-2013-5188 : Levi Musters

- **Screen Sharing Server**

  Impact: A remote attacker may be able to cause arbitrary code execution

  Description: A format string vulnerability existed in Screen Sharing Server's handling of the VNC username.

  CVE-ID

  CVE-2013-5135 : SilentSignal working with iDefense VCP

- **syslog**

  Impact: A Guest user may be able to see log messages from previous Guests

  Description: The console log was visible to the Guest user and contained messages from previous Guest user sessions. This issue was addressed by making the console log for Guest users visible only to administrators.

  CVE-ID

  CVE-2013-5191 : Sven-S. Porst of earthlingsoft

- **USB**

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

  Description: The USB hub controller didn't check the port and port number of requests. The issue was addressed by adding checks of the port and port number.

  CVE-ID

  CVE-2013-5192 : Stefano Bianchi Mazzone, Mattia Pagnozzi, and Aristide Fattori of Computer and Network Security Lab (LaSER), Università degli Studi di Milano

Note: OS X Mavericks includes Safari 7.0, which incorporates the security content of Safari 6.1. For further details see "About the security content of Safari 6.1" at http://http//support.apple.com/kb/HT6000

Last Modified: Oct 23, 2013

Additional Product Support Information