About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004

This document describes the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004.

These can be downloaded and installed via Software Update preferences, or from Apple Downloads.

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 Mountain Lion v10.8.5 and Security Update 2013-004

- **Apache**

  Available for: Mac OS X v10.6.8, Mac OS X Server v10.6.8, OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8 to v10.8.4

  Impact: Multiple vulnerabilities in Apache

  Description: Multiple vulnerabilities existed in Apache, the most serious of which may lead to cross-site scripting. These issues were addressed by updating Apache to version 2.2.24.

  CVE-ID

  CVE-2012-0883

  CVE-2012-2687

  CVE-2012-3499

  CVE-2012-4558

- **Bind**

  Available for: OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8 to v10.8.4

  Impact: Multiple vulnerabilities in BIND

  Description: Multiple vulnerabilities existed in BIND, the most serious of which may lead to a denial of service. These issues were addressed by updating BIND to version 9.8.5-P1. CVE-2012-5688 did not affect Mac OS X v10.7 systems.

  CVE-ID

  CVE-2012-3817

  CVE-2012-4244

  CVE-2012-5166

  CVE-2012-5688

  CVE-2013-2266

- **Certificate Trust Policy**

  Available for: Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8 to v10.8.4

  Impact: Root certificates have been updated

  Description: Several certificates were added to or removed from the list of system roots. The complete list of recognized system roots may be viewed via the Keychain Access application.

- **ClamAV**

  Available for: Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7.5, OS X Lion Server v10.7.5

  Impact: Multiple vulnerabilities in ClamAV

  Description: Multiple vulnerabilities exist in ClamAV, the most serious of which may lead to arbitrary code execution. This update addresses the issues by updating ClamAV to version 0.97.8.

  CVE-ID

  CVE-2013-2020

  CVE-2013-2021

- **CoreGraphics**

  Available for: OS X Mountain Lion v10.8 to v10.8.4

  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

- **ImageIO**

  Available for: OS X Mountain Lion v10.8 to v10.8.4

  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

- **Installer**

  Available for: OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8 to v10.8.4

  Impact: Packages could be opened after certificate revocation

  Description: When Installer encountered a revoked certificate, it would present a dialog with an option to continue. The issue was addressed by removing the dialog and refusing any revoked package.

  CVE-ID

  CVE-2013-1027

- **IPSec**

  Available for: Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8 to v10.8.4

  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 properly checking the certificate.

  CVE-ID

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

- **Kernel**

  Available for: OS X Mountain Lion v10.8 to v10.8.4

  Impact: A local network user may cause a denial of service

  Description: An incorrect check in the IGMP packet parsing code in the kernel allowed a user who could send IGMP packets to the system to cause a kernel panic. The issue was addressed by removing the check.

CVE-ID

CVE-2013-1029 : Christopher Bohn of PROTECTSTAR INC.

- **Mobile Device Management**

  Available for: OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8 to v10.8.4

  Impact: Passwords may be disclosed to other local users

  Description: A password was passed on the command-line to mdmclient, which made it visible to other users on the same system. The issue was addressed by communicating the password through a pipe.

  CVE-ID

  CVE-2013-1030 : Per Olofsson at the University of Gothenburg

- **OpenSSL**

  Available for: Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8 to v10.8.4

  Impact: Multiple vulnerabilities in OpenSSL

  Description: Multiple vulnerabilities existed in OpenSSL, the most serious of which may lead to disclosure of user data. These issues were addressed by updating OpenSSL to version 0.9.8y.

  CVE-ID

  CVE-2012-2686

  CVE-2013-0166

  CVE-2013-0169

- **PHP**

  Available for: Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8 to v10.8.4

  Impact: Multiple vulnerabilities in PHP

  Description: Multiple vulnerabilities existed in PHP, the most serious of which may lead to arbitrary code execution. These issues were addressed by updating PHP to version 5.3.26.

  CVE-ID

  CVE-2013-1635

  CVE-2013-1643

  CVE-2013-1824

  CVE-2013-2110

- **PostgreSQL**

  Available for: OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8 to v10.8.4

  Impact: Multiple vulnerabilities in PostgreSQL

  Description: Multiple vulnerabilities exist in PostgreSQL, the most serious of which may lead to data corruption or privilege escalation. CVE-2013-1901 does not affect OS X Lion systems. This update addresses the issues by updating PostgreSQL to version 9.1.9 on OS X Mountain Lion systems, and 9.0.4 on OS X Lion systems.

  CVE-ID

  CVE-2013-1899

  CVE-2013-1900

  CVE-2013-1901

- **Power Management**

  Available for: OS X Mountain Lion v10.8 to v10.8.4

Impact: The screen saver may not start after the specified time period

Description: A power assertion lock issue existed. This issue was addressed through improved lock handling.

CVE-ID

CVE-2013-1031

- **QuickTime**

  Available for: Mac OS X 10.6.8, Mac OS X Server 10.6.8, OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8 to v10.8.4

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

  Description: A memory corruption issue existed in the handling of 'idsc' atoms in QuickTime movie files. This issue was addressed through additional bounds checking.

  CVE-ID

  CVE-2013-1032 : Jason Kratzer working with iDefense VCP

- **Screen Lock**

  Available for: OS X Mountain Lion v10.8 to v10.8.4

  Impact: A user with screen sharing access may be able to bypass the screen lock when another user is logged in

  Description: A session management issue existed in the screen lock's handling of screen sharing sessions. This issue was addressed through improved session tracking.

  CVE-ID

  CVE-2013-1033 : Jeff Grisso of Atos IT Solutions, Sébastien Stormacq

- **sudo**

  Available for: OS X Lion v10.7.5, OS X Lion Server v10.7.5, OS X Mountain Lion v10.8 to v10.8.4

  Impact: An attacker with control of an admin user's account may be able to gain root privileges without knowing the user's password

  Description: By setting the system clock, an attacker may be able to use sudo to gain root privileges on systems where sudo has been used before. On OS X, only admin users can change the system clock. This issue was addressed by checking for an invalid timestamp.

  CVE-ID

  CVE-2013-1775

- **Note:** OS X Mountain Lion v10.8.5 also addresses an issue in which certain Unicode strings could cause applications to unexpectedly quit.

Published Date: February 15, 2024