

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

10/23/2013

SUBJECT:

Multiple Vulnerabilities in Apple Mac OS X Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Apple's Mac OS X and Mac OS X Server that could allow remote code execution. Mac OS X and Mac OS X Server are operating systems for Apple computers. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file, including an email attachment, using a vulnerable version of OS X. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Apple OS X 10.8.1 to 10.8.5

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users:High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Apple Mac OS X. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file.

The vulnerabilities are as follows:

- A security-bypass vulnerability occurs due to an error in the 'socketfilterfw --blockApp' option. Specifically, this issue occurs because it fails to properly block applications from receiving network connections. [CVE-2013-5165]
- A security-bypass vulnerability that affects the LaunchServices interface. This allows an malicious application to bypass the sandbox restrictions. [CVE-2013-5179]

- A denial of service vulnerability occurs due to an improper handling of Bluetooth USB host controller interfaces. [CVE-2013-5166]
- A session-fixation vulnerability occurs due to an improper handling of session cookies. [CVE-2013-5167]
- A remote code execution vulnerability occurs due to an improper handling of log entry with an attached URL. [CVE-2013-5168]
- A memory-corruption vulnerability occurs due to an error in CoreGraphics's handling of display sleep mode. This may result in windows being visible over the lock screen. [CVE-2013-5169]
- A buffer-overflow vulnerability occurs due to an error in the handling of PDF files. [CVE-2013-5170]
- A security-bypass vulnerability exists in the CoreGraphics component. This issue is triggered when registering for a hotkey event. Specifically, this issue allows an unprivileged application to log keystrokes entered into other applications even when secure input mode is enabled. [CVE-2013-5171]
- A denial of service vulnerability occurs due to an error in the SHA-2 digest functions. Specifically, this issue occurs because of using incorrect output length for the SHA-2 family of digest functions. [CVE-2013-5172]
- A denial of service vulnerability occurs due to the kernel random number generator holding a lock while performing requests from userspace. [CVE-2013-5173]
- A denial of service vulnerability occurs due to an integer sign issue existed in the handling of tty reads. [CVE-2013-5174]
- An out of bounds read vulnerability exists due to an error in the handling of Mach-O files. [CVE-2013-5175]
- A denial of service vulnerability occurs due to an integer truncation issue exists in the handling of tty devices. [CVE-2013-5176]
- A denial of service vulnerability occurs due to improper validation of iovec structures. [CVE-2013-5177]
- A denial of service vulnerability exists due to an error in the handling of a multicast packets. [CVE-2013-5184]
- A security vulnerability exists in the LaunchServices. Specifically, this issue occurs while handling of certain unicode characters that could allow filenames to show incorrect extensions. Attack can exploit this issue by trick a user into clicking on a malicious executable. [CVE-2013-5178]
- A security vulnerability exists in Libc. Specifically, this issue occurs when the kernel random number generator (RNG) cannot access 'srandomdev()' function. Attack can exploit this issue by predict randomly generated numbers and undermine application security. [CVE-2013-5180]
- An insecure authentication weakness in Mail Accounts. Specifically, this issue exists because the Mail app choosing plaintext authentication over CRAM-MD5 when auto-configuring a mail account on arbitrary mailservers. [CVE-2013-5181]
- A security vulnerability exists within the 'Mail Header Display' component. Specifically, this issue occurs when handling an unsigned message that contains crafted multipart/signed parts. A context-dependent attacker can exploit this issue to entice a user into clicking an unsigned message. [CVE-2013-5182]
- An information-disclosure vulnerability exists because the 'Mail Networking' component sends the unencrypted data in clear text to the remote mail server. [CVE-2013-5183] Note: Successful exploit of this issue requires the Transport Layer Security to be disabled and Kerberos authentication to be enabled.
- A security vulnerability exists in OpenLDAP which may lead to weak encryption. Specifically, this issue occurs because the ldapsearch command line tool fails to properly implement the 'minssf' configuration. [CVE-2013-5185]
- A security-bypass vulnerability exists in the power assertion management that occurs due locking issue. [CVE-2013-5186]
- A security-bypass vulnerability exists because it fails to properly enforce the administrator's security preferences. Specifically, this issue is triggered because the 'Require an administrator password to access system preferences with lock icons' security setting is disabled when performing a software update or upgrade. [CVE-2013-5189]

- A security-bypass vulnerability exists when processing Smart Card certificate revocation checks. [CVE-2013-5190]
- A security Weakness exists in the Screen Lock. Specifically, this issue exists in the 'Lock Screen' command in the Keychain Status menu bar item that is due to the screen lock not engaging until after the 'Require password [amount of time] after sleep or screen saver begins' setting had passed. This Weakness may allow a local attacker gain access to the system. [CVE-2013-5187]
- A security-bypass vulnerability occurs due to to the system waking from hibernation and not prompting for a password when hibernation and autologin are enabled. [CVE-2013-5188]
- A local information-disclosure vulnerability occurs due to the system exposing the console log to Guest users. [CVE-2013-5191]
- A local denial of service vulnerability exists in USB hub controller. Specifically, this issue occurs due to the controller failing to check the port and port number while handling malformed requests. [CVE-2013-5192]

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Apple to affected systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download or open files from un-trusted websites, unknown users, or suspicious emails.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Apple:

<http://lists.apple.com/archives/security-announce/2013/Oct/msg00004.html>

Security Focus:

<http://www.securityfocus.com/advisories/30176>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5165>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5179>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5166>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5167>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5168>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5169>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5170>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5171>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5172>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5173>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5174>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5175>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5176>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5177>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5184>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5178>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5180>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5181>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5182>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5183>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5185>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5186>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5189>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5190>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5187>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5188>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5191>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5192>