

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:

09/13/2013

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 to 10.8.4
- Apple OS X 10.7.5
- Apple OS X Server 10.7.5
- Apple OS X 10.6.8
- Apple OS X Server 10.6.8

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 buffer-overflow vulnerability occurs because of improper bounds checks of user-supplied data. An attacker can exploit this issue to execute arbitrary code within the context of the affected application. [CVE-2013-1026]
- A security-bypass vulnerability occurs because the affected application fails to restrict installation when a revoked certificate is presented. An attacker can exploit this issue to gain unauthorized access to the application, which can lead to further attacks. [CVE-2013-1027]
- A security-bypass vulnerability occurs because Mac OS X fails to properly validate the DNS name of an "IPSec Hybrid Auth" server in a signed certificate. An attacker can exploit this issue

to perform man-in-the-middle attacks or impersonate trusted servers. This can allow for the interception of data by the attacker. [CVE-2013-1028]

- A remote memory-corruption vulnerability occurs when handling the “idsc” atoms (Image description) in specially crafted QuickTime movie files. An attacker can exploit this issue to execute arbitrary code in the context of the application. A failed attempt at exploitation could result in denial-of-service conditions. [CVE-2013-1032]
- A local information-disclosure vulnerability occurs because the password for the Mobile Device Management (mdmclient) is passed through the command-line interface. A local attacker could leverage this issue to gain access to sensitive information. [CVE-2013-1030]
- A local security-bypass vulnerability can occur because of a session management error in the screen lock’s handling of screen sharing sessions. A local attacker can exploit this issue to gain unauthorized access to the system. [CVE-2013-1033]
- A denial-of-service vulnerability can occur when processing certain Unicode strings. An attacker can exploit this issue to cause the application to quit unexpectedly.
- A remote denial-of-service vulnerability can occur within the Kernel component. This is possible because the component fails to properly check the IGMP packet when parsing code. An attacker can exploit this issue to cause denial-of-service conditions. [CVE-2013-1029]

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://support.apple.com/kb/HT5880>

Security Focus:

<http://www.securityfocus.com/bid/62369>

<http://www.securityfocus.com/bid/62370>

<http://www.securityfocus.com/bid/62371>

<http://www.securityfocus.com/bid/62375>

<http://www.securityfocus.com/bid/62377>

<http://www.securityfocus.com/bid/62378>

<http://www.securityfocus.com/bid/62381>

<http://www.securityfocus.com/bid/62382>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1026>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1027>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1028>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1029>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1030>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1032>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1033>