

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:

06/05/2013

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 versions prior to 10.8.4 are vulnerable
- Apple OS X 10.7.5
- Apple OS X 10.6.8
- Apple OS X Server versions prior to 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 security-bypass vulnerability occurs when SMB file sharing is enabled. An authenticated attacker can exploit this issue to write files outside the shared directory. [CVE-2013-0990]
- A remote buffer-overflow vulnerability occurs because it fails to properly handle PICT images. [CVE-2013-0975]
- A security-bypass vulnerability occurs because as attacker with access to a user's session may be able to log into previously accessed sites. An attacker can exploit this issue even if Private Browsing was used. [CVE-2013-0982]
- A remote-code execution issue affects the text glyphs because of an unbounded stack allocation when handling maliciously crafted URLs. [CVE-2013-0983]
- A remote buffer-overflow vulnerability that occurs in the Directory Service daemon. An attacker can leverage this issue to execute arbitrary code within the context of the application. [CVE-2013-0984]
- A remote-code execution vulnerability occurs because it fails to properly handle text tracks. [CVE-2013-1024]
- A local security-bypass vulnerability affects the Disk Management component of Mac OS X 10.8.3. This issue can be exploited by an unauthorized attacker to allow FileVault to be disabled using the command-line. [CVE-2013-0985]

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.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.

- 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/HT5784>

Security Focus:

<http://www.securityfocus.com/bid/60329>

<http://www.securityfocus.com/bid/60331>

<http://www.securityfocus.com/bid/60328>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0990>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0975>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0982>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0983>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0984>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1024>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0985>