

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:

03/15/2013

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 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 Mac OS X 10.6
- Apple Mac OS X Server 10.6
- Apple Mac OS X 10.7
- Apple Mac OS X Server 10.7
- Apple Mac OS X 10.8 prior to 10.8.3
- Apple Mac OS X Server 10.8 prior to 10.8.3

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. The details of these vulnerabilities are as follows:

- An authentication-bypass issue occurs due to an error in the handling of URIs with ignorable Unicode character sequences. An attacker can exploit this issue to access directories that are protected with HTTP authentication. (CVE-2013-0966)
- A security vulnerability that allows Java Web Start applications to be launched automatically even if the Java plug-in is disabled when visiting specially crafted websites. (CVE-2013-0967)
- A memory corruption issue occurs due to an error in the handling of graphics data. An attacker can exploit this issue to execute arbitrary code within the context of affected application.(CVE-2013-0976)
- A local security-bypass vulnerability occurs due to a logic error in the VoiceOver's handling of the Login Window. An attacker with access to the keyboard could launch system preferences and modify the system configuration. (CVE-2013-0969)
- A security-bypass vulnerability occurs when clicking on a specifically-formatted 'FaceTime:/' URL in messages. An attacker can exploit this issue to initiate a FaceTime call without prompting. (CVE-2013-0970)
- A use after free issue exists due to an error in the handling of ink annotations in PDF files. (CVE-2013-0971)
- A remote code execution vulnerability occurs due to an error in the Software Update feature. An attacker can exploit this issue to insert plugin content into the marketingtext displayed for updates. (CVE-2013-0973)
- A security-bypass vulnerability occurs due to an error in several intermediate CA certificates issued by TURKTRUST.

Successful exploitation of these vulnerabilities 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. Failed attempts could result in a denial-of-service.

RECOMMENDATIONS:

We recommend the following actions 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.
- Permit local access for trusted individuals only. Where possible, use restricted environments and restricted shells.
- 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/HT5672>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0966>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0967>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0969>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0970>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0971>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0973>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0976>

SecurityFocus:

<http://www.securityfocus.com/bid/58494>