

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:

07/02/2014

SUBJECT:

Multiple Vulnerabilities in Apple Mac OS X Prior to 10.9.4

OVERVIEW:

Multiple vulnerabilities have been discovered in Apple's Mac OS X prior to 10.9.4. Mac OS X is an operating system 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, remote code execution within the context of the application, and bypass of security systems. Failed attacks may cause a Denial of Service condition within the targeted delivery method. 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.

THREAT INTELLIGENCE

There is not any known proof-of-concept code available at this time.

SYSTEMS AFFECTED:

- Apple OS X prior to 10.9.4

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 below vulnerabilities have been fixed in Security Update 2014-003.

The vulnerabilities are as follows:

- Arbitrary code-execution vulnerability affects the 'copyfile' component. Specifically, this issue occurs due to an out-of-bounds byte swapping issue in the handling of AppleDouble files in zip archives. An attacker can exploit this issue through a crafted zip file. [CVE-2014-1370]
- An arbitrary code-execution vulnerability affects the 'Dock' component. Specifically, this issue occurs due to an invalidated array index issue in the Dock's handling of messages from applications. An attacker can exploit this issue to circumvent sandbox restrictions. [CVE-2014-1371]
- An out-of-bounds read error exists in the handling of a system call. Specifically, this issue affects the 'Graphics Driver' component. A local attacker can exploit this issue to bypass the kernel address space layout randomization. [CVE-2014-1372]
- An information-disclosure vulnerability affects the 'iBooks Commerce' component. Specifically, this issue exists in the handling of iBooks logs. An attacker can exploit this issue to recover Apple ID credentials. [CVE-2014-1317]
- An arbitrary code-execution vulnerability affects the 'Intel Graphics Driver' component. Specifically, this issue occurs due to a validation issue in the handling of an OpenGL API call. An attacker can exploit this issue to execute arbitrary code with system privileges using malicious application. [CVE-2014-1373]
- A security-bypass vulnerability affects the 'Intel Graphics Driver' component. Specifically, this issue occurs because of improper handling of a kernel pointer stored in an IOKit object. A local attacker can exploit this issue to bypass the kernel address space layout randomization. [CVE-2014-1375]
- An arbitrary code-execution vulnerability affects the 'Intel Compute' component. Specifically, this issue occurs due to a validation issue in the handling of an OpenCL API call. An attacker can exploit this issue to execute arbitrary code with system privileges using malicious application. [CVE-2014-1376]
- An arbitrary code-execution vulnerability affects the 'IOAcceleratorFamily' component. Specifically, this issue occurs due to an array indexing issue in IOAcceleratorFamily. An attacker can exploit this issue to execute arbitrary code with system privileges using malicious application. [CVE-2014-1377]
- A local security-bypass vulnerability issue exists in the 'IOGraphicsFamily' component. Specifically, this issue occurs due to improper handling of kernel pointer stored in an IOKit object. An attacker can exploit this issue to bypass kernel address space layout randomization. [CVE-2014-1378]
- Multiple privilege-escalation vulnerabilities occur due to multiple null dereference issues in the kernel graphics drivers. An attacker can exploit these issues to gain elevated privileges through a crafted 32-bit executable. [CVE-2014-1379]

- A local security-bypass vulnerability issue exists in the 'Security - Keychain' component. Specifically, this issue occurs due to improper handling of keystroke observer management. an attacker can exploit this issue to to type into windows under the screen lock. [CVE-2014-1380]
- An out-of-bounds memory access issue exists due to improper handling of IOThunderBoltController API calls. An attacker can exploit this issue to execute arbitrary code with system privileges using malicious application. [CVE-2014-1381]

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/HT1222>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1317>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1370>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1371>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1372>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1373>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1374>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1375>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1376>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1377>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1378>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1379>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1380>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1381>