

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.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>

DATE(S) ISSUED:

03/10/2015

03/23/2015 - UPDATED

SUBJECT:

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

OVERVIEW

Multiple vulnerabilities have been discovered in Apple MAC OS X. 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 no known proof-of-concept code available at this time. Updates are available.

SYSTEM AFFECTED:

- Apple Mac OS X Yosemite v10.10.2
- Apple Mac OS X Mavericks v10.9.5
- Apple Mac OS X Mountain Lion v10.8.5

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

TECHNICAL SUMMARY:

Multiple remote code execution vulnerabilities have been discovered in Mac OS X that could allow remote code execution. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file. Details of these vulnerabilities are as follows:

- Apple Mac OS X Yosemite v10.10.2 is prone to multiple buffer overflows resulting from the handling of data during iCloud Keychain recovery (CVE-2015-1065).

- Apple Mac OS X Yosemite v10.10.2 is prone leaked kernel addresses and heap permutation values resulting from the match_port_kobject kernel interface (CVE-2015-1066).
- Apple OS X Mountain Lion v10.8.5, OS X Mavericks v10.9.5, and OS X Yosemite v10.10.2 are prone to an off by one issue in the IOAcceleratorFamily (CVE-2015-1061).
- Apple OS X Mountain Lion v10.8.5, OS X Mavericks v10.9.5, and OS X Yosemite v10.10.2 are prone to a type confusion issue with IOSurface's handling of serialized objects (CVE-2014-4496).
- Apple OS X Mountain Lion v10.8.5, OS X Mavericks v10.9.5, and OS X Yosemite v10.10.2 are prone accepting short ephemeral RSA keys, also known as FREAK attack (CVE-2015-1067).

MARCH 21 – UPDATED TECHNICAL SUMMARY:

Apple noted that multiple vulnerabilities for Apple OSX Yosemite v10.10.2 were not addressed in Apple Security Update 2015-002. The following vulnerabilities were addressed in Apple Security Update 2015-003:

- **Apple Mac OS X Yosemite v10.10.2 is prone to multiple buffer overflows resulting from the handling of data during iCloud Keychain recovery (CVE-2015-1065).**
- **Apple OS X Mountain Lion v10.8.5, OS X Mavericks v10.9.5, and OS X Yosemite v10.10.2 are prone to an off by one issue in the IOAcceleratorFamily (CVE-2015-1061).**

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate updates provided by Apple to vulnerable 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, accept, or execute files from un-trusted or unknown sources.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

MARCH 21 – UPDATED RECOMMENDATIONS:

The following actions should be taken:

- **Apply updates from Apple Security Update 2015-003 to vulnerable systems immediately after appropriate testing.**

REFERENCES:

Apple:

<https://support.apple.com/en-us/HT204413>

SecurityFocus:

<http://www.securityfocus.com/advisories/34966>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4496>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1061>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1065>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1066>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1067>

MARCH 21 UPDATED REFERENCES:

Apple:

<https://support.apple.com/en-us/HT204563>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>