

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 ISSUED:

01/28/2015

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 that could allow for remote code execution. 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 of these vulnerabilities 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.

THREAT INTELLIGENCE:

There is no known proof-of-concept code available at this time. Updates are available.

SYSTEM AFFECTED:

- Apple OS X prior to 10.10.2

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 vulnerabilities have been discovered in Apple Mac OS X, prior to version 10.10.2. 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 Updates 2015-003. The vulnerabilities are as follows:

- A remote attacker may be able to determine all the network addresses of the system [CVE-2014-4426].
- Multiple vulnerabilities in bash, including one that may allow local attackers to execute arbitrary code [CVE-2014-6277], [CVE-2014-7186], and [CVE-2014-7187].
- A malicious application may be able to execute arbitrary code with system privileges [CVE-2014-4497], [CVE-2014-8836], [CVE-2014-8837], [CVE-2014-8817],[CVE-2014-4486],[CVE-2014-4487],[CVE-2014-4488],[CVE-2014-4489],[CVE-2014-4389], [CVE-2014-4495], [CVE-2014-8824], and [CVE-2014-4461].

- Website cache may not be fully cleared after leaving private browsing [CVE-2014-4460].
- Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution [CVE-2014-4481], [CVE-2014-8816], and [CVE-2014-4483].
- A malicious Thunderbolt device may be able to affect firmware flashing [CVE-2014-4498].
- An attacker with access to a system may be able to recover Apple ID credentials [CVE-2014-4499].
- Some third-party applications with non-secure text entry and mouse events may log those events [CVE-2014-1595].
- Processing a maliciously crafted .dfont file may lead to an unexpected application termination or arbitrary code execution [CVE-2014-4484].
- Viewing a maliciously crafted XML file may lead to an unexpected application termination or arbitrary code execution [CVE-2014-4485].
- Multiple vulnerabilities existed in the Intel graphics driver, the most serious of which may have led to arbitrary code execution with system privileges. [CVE-2014-8819], [CVE-2014-8820], and [CVE-2014-8821].
- Executing a malicious application may result in arbitrary code execution within the kernel [CVE-2014-8822].
- A privileged application may be able to read arbitrary data from kernel memory [CVE-2014-8823].
- A local attacker can spoof directory service responses to the kernel, elevate privileges, or gain kernel execution [CVE-2014-8825].
- A local user may be able to determine kernel memory layout [CVE-2014-4371], [CVE-2014-4419], [CVE-2014-4420], and [CVE-2014-4421].
- A person with a privileged network position may cause a denial of service [CVE-2011-2391].
- Maliciously crafted or compromised applications may be able to determine addresses in the kernel [CVE-2014-4491].
- A malicious JAR file may bypass Gatekeeper checks [CVE-2014-8826].
- A malicious, sandboxed app can compromise the networkd daemon [CVE-2014-4492].
- A Mac may not lock immediately upon wake [CVE-2014-8827].
- Using the command line ftp tool to fetch files from a malicious http server may lead to arbitrary code execution [CVE-2014-8517].
- Multiple vulnerabilities in OpenSSL 0.9.8za, including one that may allow an attacker to downgrade connections to use weaker cipher-suites in applications using the library [CVE-2014-3566], [CVE-2014-3567], and [CVE-2014-3568].
- A sandboxed process may be able to circumvent sandbox restrictions [CVE-2014-8828].
- A malicious application could execute arbitrary code leading to compromise of user information [CVE-2014-8829].
- Viewing a maliciously crafted Collada file may lead to an unexpected application termination or arbitrary code execution [CVE-2014-8830].
- A downloaded application signed with a revoked Developer ID certificate may pass Gatekeeper checks [CVE-2014-8838].
- An app may access keychain items belonging to other apps [CVE-2014-8831].
- The sender of an email could determine the IP address of the recipient [CVE-2014-8839].
- Spotlight may save unexpected information to an external hard drive [CVE-2014-8832].
- Spotlight may display results for files not belonging to the user [CVE-2014-8833].
- A malicious application may be able to execute arbitrary code with root privileges [CVE-2014-8835].
- Printing-related preference files may contain sensitive information about PDF documents [CVE-2014-8834].

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://lists.apple.com/archives/security-announce/2015/Jan/msg00003.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2391>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1595>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3567>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3568>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4371>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4389>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4419>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4420>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4421>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4426>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4460>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4461>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4481>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4483>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4484>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4485>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4486>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4487>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4488>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4489>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4491>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4492>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4495>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4497>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4498>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4499>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6277>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7186>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7187>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8517>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8816>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8817>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8819>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8820>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8821>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8822>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8823>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8824>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8825>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8826>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8827>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8828>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8829>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8830>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8831>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8832>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8833>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8834>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8835>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8836>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8837>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8838>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8839>

SecurityFocus:

<http://www.securityfocus.com/advisories/34713>

<http://www.securityfocus.com/bid/72328>

TLP:WHITE

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

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