

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:

05/05/2015

SUBJECT:

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

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Apple MAC OS X and Apple Safari. Mac OS X is an operating system for Apple computers. Apple Safari is a web browser available for Mac OS X and Microsoft Windows. 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.

SYSTEMS AFFECTED:

Apple Mac OS X Yosemite prior to v10.10.3

Apple Mac OS X Mavericks v10.9.5

Apple Mac OS X Mountain Lion v10.8.5

Apple Safari v8.0.5, 7.1.5, and 6.2.5

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 prior to v10.10.2 is prone to privilege escalation due to an issue with checking XPC entitlements (CVE-2015-1130).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 have multiple vulnerabilities in Apache prior to versions 2.4.10 and 2.2.29 including one that may allow a remote attacker to execute arbitrary code (CVEs 2015-1066, 2013-5704, 2013-6438, 2014-0098, 2014-0117, 2014-0118, 2014-0226, and 2014-0231).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion 10.8.5, and OS X Mavericks v10.9.5 ATS (Apple Type Services) are prone to multiple input validation issues in fontd which may allow a local user to execute arbitrary code with system privileges (CVEs 2015-1131, 2015-1132, 2015-1133, 2015-1134, and 2015-1135).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to a cross-domain cookie issue which may result in cookies belonging to one origin may be sent to another origin (CVE-2015-1089).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to a cross-domain HTTP request issue which may result in authentication credentials being sent to a server on another origin (CVE-2015-1091).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to an input validation issue which may result in the execution of arbitrary code by visiting a maliciously crafted website (CVE-2015-1088).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to a use-after-free issue in CoreAnimation which may result in the execution of arbitrary code by visiting a maliciously crafted website (CVE-2015-1136).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to multiple memory corruption issues in the processing of font files, which may result in the execution of arbitrary code by processing a maliciously crafted font file (CVE-2015-1093).

Apple Mac OS X Yosemite prior to v10.10.2 and OS X Mavericks v10.9.5 are prone to an issue with NVIDIA graphics driver's handling of certain IOService userclient types, which may allow a local user to execute arbitrary code with system privileges (CVE-2015-1137).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to an input validation issue in the hypervisor framework which may allow a local application to cause a denial of service (CVE-2015-1138).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to a memory corruption issue in the handling of .sgi files which may result in the execution of arbitrary code by processing a maliciously crafted .sgi file (CVE-2015-1139).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to a memory corruption issue which may allow a malicious HID (Human Interface Device) to cause arbitrary code execution (CVE-2015-1095).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to a buffer overflow issue which may allow a local user to execute arbitrary code with system privileges (CVE-2015-1140).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to a kernel memory content disclosure issue which may allow a local user to determine kernel memory layout (CVE-2015-1096).

Apple Mac OS X Mountain Lion v10.8.5 and OS X Mavericks v10.9.5 are prone to a heap buffer overflow in the IOHIDFamily's handling of key-mapping properties which may allow a malicious application to execute arbitrary code with system privileges (CVE-2014-4404).

Apple Mac OS X Mountain Lion v10.8.5 and OS X Mavericks v10.9.5 are prone to a null pointer dereference issue in the IOHIDFamily's handling of key-mapping properties which may allow a malicious application to execute arbitrary code with system privileges (CVE-2014-4405).

Apple Mac OS X Mountain Lion v10.8.5 and OS X Mavericks v10.9.5 are prone to an out-of-bounds issue in the IOHIDFamily driver which may allow a user to execute arbitrary code with system privileges (CVE-2014-4380).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to an issue in the handling of virtual memory operations within the kernel which may allow a local user to cause unexpected system shutdown (CVE-2015-1141).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to a race condition in the kernel's setreuid system call which may allow a local user to cause a system denial of service (CVE-2015-1099).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to setreuid and setregid system calls not dropping privileges permanently which may allow a local application to escalate privileges (CVE-2015-1117).

Apple Mac OS X Yosemite prior to v10.10.2 ICMP redirects were enabled by default, which may allow an attacker with a privileged network position to redirect user traffic to arbitrary hosts (CVE-2015-1103).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to an issue processing TCP headers which may allow an attacker with a privileged network position to cause a denial of service (CVE-2015-1102).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to an out of bounds memory access issue which may allow a local user to cause unexpected system termination or read kernel memory (CVE-2015-1100).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to improper treatment of some IPv6 packets which may allow a remote user to bypass network filters (CVE-2015-1104).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to a memory corruption issue in the kernel which may allow a local user to execute arbitrary code with kernel privileges (CVE-2015-1101).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to a state inconsistency issue in the handling of TCP out of band data which may allow a remote attacker to cause a denial of service (CVE-2015-1105).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to an input validation issue in LaunchService's handling of application localization data which may allow a local user to cause the Finder to crash (CVE-2015-1142).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to a type confusion in LaunchService's handling of

localized strings which may allow a local user to execute arbitrary code with system privileges (CVE-2015-1143).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to a memory corruption issue in the handling of configuration profiles which may allow the processing of a maliciously crafted configuration profile to cause unepxtd application termination (CVE-2015-1118).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to weak key generation in ntpd when an authentication key is not configured which may allow a remote attacker to brute force ntpd authentication keys (CVE-2014-9298).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to multiple input validation issue in OpenLDAP which may allow a remote unauthenticated client to cause a denial of service (CVEs 2015-1545 and 2015-1546).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to multiple vulnerabilities in OpenSSL 0.9.8zc, including one that may allow an attacker to intercept connections to a server that supports export-grade ciphers (CVEs 2014-3569, 2014-3570, 2014-3571, 2014-3572, 2014-8275, and 2015-0204).

Apple Mac OS X Yosemite prior to v10.10.2 and OSX Mavericks v10.9.5 are prone to an Open Directory Client issue which may allow an unencrypted password to be sent over the network when using Open Directory from OS X Server (CVE-2015-1147).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to multiple vulnerabilities in PHP, including one which may lead to arbitrary code execution (CVEs 2013-6712, 2014-0207, 2014-0237, 2014-0238, 2014-2497, 2014-3478, 2014-3479, 2014-3480, 2014-3487, 2014-3538, 2014-3587, 2014-3597, 2014-3668, 2014-3669, 2014-3670, 2014-3710, 2014-3981, 2014-4049, 2014-4670, 2014-4698, and 2014-5120).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to a memory corruption issue in the handling of iWork files which may allow an opened, maliciously crafted iWork file to execute arbitrary code (CVE-2015-1098).

Apple Mac OS X Mountain Lion v10.8.5 is prone to a heap buffer overflow which may allow viewing a maliciously crafted Collada file to lead to arbitrary code execution (CVE-2014-8830).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to an issue that may allow a user's password to be logged to a local file (CVE 2015-1148).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to an issue that may allow tampered applications to launch (CVEs 2015-1145 and 2015-1146).

Apple Mac OS X Yosemite prior to v10.10.2 is prone to a memory corruption issue in WebKit that may result in arbitrary code execution after visiting a maliciously crafted website (CVE-2015-1069).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to an issue in Safari that may allow users to be tracked by malicious websites using client certificates (CVE-2015-1129).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to an issue in Safari that may allow user's browsing history in private browsing mode to be revealed (CVE-2015-1128).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to an issue in Safari that will cause the incomplete purging of a user's browsing history (CVE-2015-1112).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to multiple memory corruption issues in WebKit that may result in unexpected application termination or arbitrary code execution after visiting a maliciously crafted website (CVEs 2015-1119, 2015-1120, 2015-1121, 2015-1122, and 2015-1124).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to a state management issue that may result in a user's browsing history in private mode being indexed (CVE-2015-1127).

Apple Mac OS X Yosemite prior to v10.10.2, OS X Mountain Lion v10.8.5, and OS X Mavericks v10.9.5 are prone to an issue in WebKit's credential handling for FTP URLs that may result in resources of another origin being accessed after visiting a maliciously crafted website (CVE-2015-1126).

Security Update 2015-004 (available for OS X Mountain Lion v10.8.5 and OS X Mavericks v10.9.5) also addresses an issue caused by the fix for CVE-2015-1067 in Security Update 2015-002. This issue prevented Remote Apple Events clients on any version from connecting to the Remote Apple Events server. In default configurations, Remote Apple Events is not enabled.

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.

RECOMMENDATIONS:

The following actions should be taken:

Upgrade to Apple Mac OS X Yosemite 10.10.3 immediately after appropriate testing.

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.

REFERENCES:

Apple:

<https://support.apple.com/en-us/HT204659>

<https://support.apple.com/en-us/HT204658>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1130>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5704>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-6438>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3587>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3597>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3668>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3669>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3670>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3710>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3981>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4049>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4670>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4698>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5120>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1098>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8830>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1148>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1145>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1146>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1144>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1069>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1129>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1128>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1112>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1119>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1120>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1121>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1122>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1124>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1127>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1126>

TLP: WHITE

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

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