

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:

12/08/2015

SUBJECT:

Multiple Vulnerabilities in Apple Products Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in OS X, Safari, iOS, watchOS, tvOS, and Xcode. OS X is an operating system for Apple computers. Apple Safari is a web browser available for OS X and Microsoft Windows. Apple iOS is an operating system for iPhone, iPod touch, and iPad. Apple watchOS is an operating system for Apple Watch. Apple tvOS is an operating system for Apple TV. Xcode is a development tool for creating iOS, watchOS, and tvOS applications. 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.

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, or the bypassing of security restrictions. Failed attacks may still 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 are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- OS X El Capitan prior to 10.11.2
- Safari prior to 9.0.2
- iOS prior to 9.2
- watchOS prior to 2.1
- tvOS prior to 9.1
- Xcode prior to 7.2

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 OS X, Safari, iOS, watchOS, tvOS, and Xcode. The most serious of these vulnerabilities could lead to remote code execution. Details of all vulnerabilities are as follows:

- Multiple vulnerabilities exist in PHP versions prior to 5.5.29, the most serious of which may allow remote code execution. These vulnerabilities are addressed by updating PHP to version 5.5.30. (CVE-2015-7803, CVE-2015-7804)
- An issue exists in the sandbox's handling of hard links. This issue was addressed through improved hardening of the app sandbox. (CVE-2015-7001)
- A memory corruption issue exists in the Bluetooth HCI interface. This issue was addressed through improved memory handling. (CVE-2015-7108)
- An input validation issue exists within URL processing. This issue was addressed through improved URL validation. (CVE-2015-7094)
- An uninitialized memory access issue exists in zlib. This issue was addressed through improved memory initialization and additional validation of zlib streams. (CVE-2015-7054)
- An issue exists when installing configuration profiles. This issue was addressed through improved authorization checks. (CVE-2015-7062)
- A memory corruption issue exists in the processing of font files. This issue was addressed through improved input validation. (CVE-2015-7105)
- Multiple memory corruption issues exist in the processing of malformed media files. These issues were addressed through improved memory handling. (CVE-2015-7074, CVE-2015-7075)
- A memory corruption issue exists in the parsing of disk images. This issue was addressed through improved memory handling. (CVE-2015-7110)
- A path validation issue exists in the kernel loader. This was addressed through improved environment sanitization. (CVE-2015-7063)
- A path validation issue exists in app scoped bookmarks. This was addressed through improved environment sanitization. (CVE-2015-7071)
- A use after free issue exists in the handling of VM objects. This issue was addressed through improved memory management. (CVE-2015-7078)
- An XML external entity reference issue exists with iBook parsing. This issue was addressed through improved parsing. (CVE-2015-7081)
- A null pointer dereference issue was addressed through improved input validation. (CVE-2015-7076)
- A memory corruption issue exists in the Intel Graphics Driver. This issue was addressed through improved memory handling. (CVE-2015-7106)
- An out of bounds memory access issue exists in the Intel Graphics Driver. This issue was addressed through improved memory handling. (CVE-2015-7077)
- A memory corruption issue exists in IOAcceleratorFamily. This issue was addressed through improved memory handling. (CVE-2015-7109)
- Multiple memory corruption issues exist in IOHIDFamily API. These issues were addressed through improved memory handling. (CVE-2015-7111, CVE-2015-7112)
- A null pointer dereference exists in the handling of a certain userclient type. This issue was addressed through improved validation. (CVE-2015-7068)
- A null pointer dereference exists in IOTThunderboltFamily's handling of certain userclient types. This issue was addressed through improved validation of IOTThunderboltFamily contexts. (CVE-2015-7067)
- Multiple denial of service issues were addressed through improved memory handling. (CVE-2015-7040, CVE-2015-7041, CVE-2015-7042, CVE-2015-7043)
- Multiple memory corruption issues exist in the kernel. These issues were addressed through improved memory handling. (CVE-2015-7083, CVE-2015-7084)
- An issue exists in the parsing of mach messages. This issue was addressed through improved validation of mach messages. (CVE-2015-7047)

- A validation issue exists during the loading of kernel extensions. This issue was addressed through additional verification. (CVE-2015-7052)
- An issue exists in how Keychain Access interacted with Keychain Agent. This issue was resolved by removing legacy functionality. (CVE-2015-7045)
- A memory corruption issue exists in the processing of archives. This issue was addressed through improved memory handling. (CVE-2011-2895)
- Multiple buffer overflows exist in the C standard library. These issues were addressed through improved bounds checking. (CVE-2015-7038, CVE-2015-7039)
- Multiple vulnerabilities exist in expat version prior to 2.1.0. These were addressed by updating expat to versions 2.1.0. (CVE-2012-0876, CVE-2012-1147, CVE-2012-1148)
- A memory corruption issue exists in the parsing of XML files. This issue was addressed through improved memory handling. (CVE-2015-3807)
- Multiple memory corruption issues exist in OpenGL. These issues were addressed through improved memory handling. (CVE-2015-7064, CVE-2015-7065, CVE-2015-7066)
- An input validation issue exists in OpenLDAP. This issue was addressed through improved input validation. (CVE-2015-6908)
- Multiple vulnerabilities exist in LibreSSL versions prior to 2.1.8. These were addressed by updating LibreSSL to version 2.1.8. (CVE-2015-5333, CVE-2015-5334)
- A memory corruption issue exists in the handling of iWork files. This issue was addressed through improved memory handling. (CVE-2015-7107)
- An insufficient privilege separation issue exists in xnu. This issue was addressed by improved authorization checks. (CVE-2015-7046)
- A memory corruption issue exists in handling SSL handshakes. This issue was addressed through improved memory handling. (CVE-2015-7073)
- Multiple memory corruption issues exist in the ASN.1 decoder. These issues were addressed through improved input validation (CVE-2015-7059, CVE-2015-7060, CVE-2015-7061)
- An issue exists in the validation of access control lists for keychain items. This issue was addressed through improved access control list checks. (CVE-2015-7058)
- A privilege issue exists in handling union mounts. This issue was addressed by improved authorization checks. (CVE-2015-7044)
- Multiple memory corruption issues exist in WebKit. These issues were addressed through improved memory handling. (CVE-2015-7048, CVE-2015-7095, CVE-2015-7096, CVE-2015-7097, CVE-2015-7098, CVE-2015-7099, CVE-2015-7100, CVE-2015-7101, CVE-2015-7102, CVE-2015-7103, CVE-2015-7104)
- An insufficient input validation issue exists in content blocking. This issue was addressed through improved content extension parsing. (CVE-2015-7050)
- An access control issue was addressed by preventing modification of access control structures. (CVE-2015-7055)
- Multiple segment validation issues exist in dyld. These were addressed through improved environment sanitization. (CVE-2015-7072, CVE-2015-7079)
- Multiple path validation issues exist in Mobile Replayer. These were addressed through improved environment sanitization. (CVE-2015-7069, CVE-2015-7070)
- A memory corruption issue exists in the processing of malformed plists. This issue was addressed through improved memory handling. (CVE-2015-7113)
- A timing issue exists in loading of the trust cache. This issue was resolved by validating the system environment before loading the trust cache. (CVE-2015-7051)
- A path validation issue exists in Mobile Backup. This was addressed through improved environment sanitization. (CVE-2015-7037)
- An issue may have allowed a website to display content with a URL from a different website. This issue was addressed through improved URL handling. (CVE-2015-7093)

- When a request was made to Siri, client side restrictions are not being checked by the server. This issue was addressed through improved restriction checking. (CVE-2015-7080)
- A memory corruption issue exists in ImageIO. This issue was addressed through improved memory handling. (CVE-2015-7053)
- Multiple memory corruption issues exist in the processing of font files. These issues were addressed through improved bounds checking. (CVE-2015-6978)
- A memory corruption issue exists in the kernel. This issue was addressed through improved memory handling. (CVE-2015-6979)
- The kSecRevocationRequirePositiveResponse flag was specified but not implemented. This issue was addressed by implementing the flag. (CVE-2015-6997)
- Multiple vulnerabilities exist in Git versions prior to 2.5.4. These were addressed by updating Git to version 2.5.4. (CVE-2015-7082)
- Xcode does not honor the .gitignore directive. This issue was addressed by adding support to honor .gitignore file. (CVE-2015-7056)
- Multiple memory corruption issues exist in the processing of mach-o files. These issues were addressed through improved memory handling. (CVE-2015-7049, CVE-2015-7057)

Successful exploitation of the most serious 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, or the ability to bypass the security system. 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 updates provided by Apple to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user 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/kb/HT205642>
<https://support.apple.com/kb/HT205639>
<https://support.apple.com/kb/HT205641>
<https://support.apple.com/kb/HT205637>
<https://support.apple.com/kb/HT205640>
<https://support.apple.com/kb/HT205635>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2895>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0876>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1147>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1148>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3807>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5333>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5334>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6908>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6978>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6979>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6997>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7094>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7095>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7096>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7097>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7098>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7099>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7100>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7101>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7102>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7103>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7104>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7105>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7106>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7107>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7108>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7109>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7110>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7111>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7112>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7113>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7803>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7804>

TLP: WHITE

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

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