



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

October 22, 2015

The following cyber advisory was issued by the State of Alaska and was 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.

ADVISORY NUMBER:

SA2015-126

DATE(S) ISSUED:

10/22/2015

SUBJECT:

Multiple Vulnerabilities in Apple Products Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in OS X, iTunes, Safari, iOS, and watchOS. OS X is an operating system for Apple computers. Apple iTunes is used to play media files on Microsoft Windows and MAC OS X platforms. 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. 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, and bypassing 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 Mavericks prior to 10.9.5

- OS X Yosemite prior to 10.10.5
- OS X El Capitan prior to 10.11
- iTunes prior to 12.3.1
- Safari prior to 9.0.1
- iOS prior to 9.1
- watchOS prior to 2.0.1

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 iOS, watchOS, Safari, iTunes, and OS X that could allow remote code execution. These vulnerabilities are as follows:

- An issue existed with EFI argument handling. This was addressed by removing the affected functions (CVE-2015-7035).
- Multiple memory corruption issues existed in WebKit. These issues were addressed through improved memory handling (CVE-2015-5928, CVE-2015-5929, CVE-2015-5930, CVE-2015-5931, CVE-2015-7002, CVE-2015-7011, CVE-2015-7012, CVE-2015-7013, CVE-2015-7014).
- Multiple memory corruption issues existed in the processing of text files. These issues were addressed through improved memory handling (CVE-2015-6975, CVE-2015-6992, CVE-2015-7017).
- The transaction log functionality was enabled in certain configurations. This issue was addressed by removing the transaction log functionality. This update additionally addresses the issue for Apple Watches manufactured with watchOS 2 (CVE-2015-5916).
- A file traversal vulnerability existed in the handling of CPIO archives. This issue was addressed through improved validation of metadata (CVE-2015-7006).
- A heap based buffer overflow issue existed in the DNS client library. A local user with the ability to spoof responses from the local configd service may have been able to cause arbitrary code execution in DNS clients (CVE-2015-7015).
- A memory corruption issue existed in CoreGraphics. This issue was addressed through improved memory handling (CVE-2015-5925, CVE-2015-5926).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-5927, CVE-2015-5942).
- A memory corruption issue existed in the handling of dispatch calls. This issue was addressed through improved memory handling (CVE-2015-6989).
- Multiple memory corruption issues existed in the parsing of image metadata. These issues were addressed through improved metadata validation (CVE-2015-5935, CVE-2015-5936, CVE-2015-5937, CVE-2015-5939).

- A memory corruption issue existed in IOAcceleratorFamily. This issue was addressed through improved memory handling (CVE-2015-6996).
- A memory corruption issue existed in the kernel. This issue was addressed through improved memory handling (CVE-2015-6974).
- A double free issue existed in the handling of AtomicBufferedFile descriptors. This issue was addressed through improved validation of AtomicBufferedFile descriptors (CVE-2015-6983).
- A file traversal vulnerability existed in the handling of CPIO archives. This issue was addressed through improved validation of metadata (CVE-2015-7006).
- A heap based buffer overflow issue existed in the DNS client library. A malicious application with the ability to spoof responses from the local configd service may have been able to cause arbitrary code execution in DNS clients (CVE-2015-7015).
- A memory corruption issue existed in IOAcceleratorFamily. This issue was addressed through improved memory handling (CVE-2015-6996).
- A memory corruption issue existed in OpenGL. This issue was addressed through improved memory handling (CVE-2015-5924).
- A memory corruption issue existed in the Accelerate Framework in multi-threading mode. This issue was addressed through improved accessor element validation and improved object locking (CVE-2015-5940).
- A memory corruption issue existed in the kernel. This issue was addressed through improved memory handling (CVE-2015-6974).
- A memory corruption issue existed in the kernel. This issue was addressed through improved memory handling (CVE-2015-6979).
- A memory corruption issue existed in the parsing of disk images. This issue was addressed through improved memory handling (CVE-2015-6995).
- A memory corruption issue existed when handling dispatch calls. This issue was addressed through improved memory handling (CVE-2015-6989).
- A parsing issue existed when handling cookies with different letter casing. This issue was addressed through improved parsing (CVE-2015-7023).
- A type confusion issue existed in AppleVXD393. This issue was addressed through improved memory handling (CVE-2015-6986).
- A validation issue existed in the OCSP client. This issue was addressed by checking the OCSP certificate's expiration time (CVE-2015-6999).
- An input validation issue existed in the kernel. This issue was addressed through improved input validation (CVE-2015-7004).
- An issue existed in the authorization checks for querying phone call status. This issue was addressed through additional authorization state queries (CVE-2015-7022).
- An issue existed when reusing virtual memory. This issue was addressed through improved validation (CVE-2015-6994).
- An uninitialized memory issue existed in the kernel. This issue was addressed through improved memory initialization (CVE-2015-6988).
- Multiple memory corruption issues existed in CoreGraphics. These issues were addressed through improved memory handling (CVE-2015-5925, CVE-2015-5926).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-5927, CVE-2015-5942,

CVE-2015-6976, CVE-2015-6977, CVE-2015-6978, CVE-2015-6990, CVE-2015-6991, CVE-2015-6993, CVE-2015-7008, CVE-2015-7009, CVE-2015-7010, CVE-2015-7018).

- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-6975, CVE-2015-6992, CVE-2015-7017).
- Multiple memory corruption issues existed in the parsing of image metadata. These issues were addressed through improved metadata validation (CVE-2015-5935, CVE-2015-5936, CVE-2015-5937, CVE-2015-5939).
- Multiple memory corruption issues existed in WebKit. These issues were addressed through improved memory handling (CVE-2015-5928, CVE-2015-5929, CVE-2015-5930, CVE-2015-6981, CVE-2015-6982, CVE-2015-7002, CVE-2015-7005, CVE-2015-7012, CVE-2015-7014).
- The kSecRevocationRequirePositiveResponse flag was specified but not implemented. This issue was addressed by implementing the flag (CVE-2015-6997).
- When "Show on Lock Screen" was turned off for Phone or Messages, configuration changes were not immediately applied. This issue was addressed through improved state management (CVE-2015-7000).
- A double free issue existed in the handling of AtomicBufferedFile descriptors. This issue was addressed through improved validation of AtomicBufferedFile descriptors (CVE-2015-6983).
- A file traversal vulnerability existed in the handling of CPIO archives. This issue was addressed through improved validation of metadata (CVE-2015-7006).
- A heap based buffer overflow issue existed in the DNS client library. A malicious application with the ability to spoof responses from the local configd service may have been able to cause arbitrary code execution in DNS clients (CVE-2015-7015).
- A memory corruption issue existed in ATS. This issue was addressed through improved memory handling (CVE-2015-6985).
- A memory corruption issue existed in IOAcceleratorFamily. This issue was addressed through improved memory handling (CVE-2015-6996).
- A memory corruption issue existed in OpenGL. This issue was addressed through improved memory handling (CVE-2015-5924).
- A memory corruption issue existed in the Accelerate Framework in multi-threading mode. This issue was addressed through improved accessor element validation and improved object locking (CVE-2015-5940).
- A memory corruption issue existed in the handling of dispatch calls. This issue was addressed through improved memory handling (CVE-2015-6989).
- A memory corruption issue existed in the kernel. This issue was addressed through improved memory handling (CVE-2015-6974).
- A memory corruption issue existed in the kernel. This issue was addressed through improved memory handling (CVE-2015-7021).
- A memory corruption issue existed in the parsing of disk images. This issue was addressed through improved memory handling (CVE-2015-6995).
- A method existed for applications to create synthetic clicks on keychain prompts. This was addressed by disabling synthetic clicks for keychain access windows (CVE-2015-5943).

- A parsing issue existed when handling cookies with different letter casing. This issue was addressed through improved parsing (CVE-2015-7023).
- A privilege separation issue existed in PAM support. This issue was addressed with improved authorization checks (CVE-2015-6563).
- A type confusion issue existed in the validation of Mach tasks. This issue was addressed through improved Mach task validation (CVE-2015-5932).
- An entitlement validation issue existed in Managed Configuration. A developer-signed app could bypass restrictions on use of restricted entitlements and elevate privileges. This issue was addressed through improved provisioning profile validation (CVE-2015-7016).
- An input validation issue existed in parsing bookmark metadata. This issue was addressed through improved validation checks (CVE-2015-6987).
- An input validation issue existed when handling NVRAM parameters. This issue was addressed through improved validation (CVE-2015-5945).
- An issue existed when reusing virtual memory. This issue was addressed through improved validation (CVE-2015-6994).
- An issue existed with EFI argument handling. This was addressed by removing the affected functions (CVE-2015-7035).
- An issue existed within the path validation logic for symlinks. This issue was addressed through improved path sanitization (CVE-2015-6984).
- An uninitialized memory issue existed in coreaudiod. This issue was addressed through improved memory initialization (CVE-2015-7003).
- An uninitialized memory issue existed in the kernel. This issue was addressed through improved memory initialization (CVE-2015-6988).
- In some circumstances, Script Editor did not ask for user confirmation before executing AppleScripts. This issue was addressed by prompting for user confirmation before executing AppleScripts (CVE-2015-7007).
- Multiple issues existed in netsh version 5.6. These issues were addressed by using patches affecting OS X from upstream (CVE-2012-6151, CVE-2014-3565).
- Multiple memory corruption issues existed in CoreGraphics. These issues were addressed through improved memory handling (CVE-2015-5925, CVE-2015-5926).
- Multiple memory corruption issues existed in the handling of audio files. These issues were addressed through improved memory handling (CVE-2015-5933, CVE-2015-5934).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-5927, CVE-2015-5942, CVE-2015-6976, CVE-2015-6977, CVE-2015-6978, CVE-2015-6991, CVE-2015-6993, CVE-2015-7009, CVE-2015-7010, CVE-2015-7018).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-5944).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-6975).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-6990, CVE-2015-7008).
- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-6992).

- Multiple memory corruption issues existed in the handling of font files. These issues were addressed through improved bounds checking (CVE-2015-7017).
- Multiple memory corruption issues existed in the parsing of image metadata. These issues were addressed through improved metadata validation (CVE-2015-5935, CVE-2015-5938).
- Multiple memory corruption issues existed in the parsing of image metadata. These issues were addressed through improved metadata validation (CVE-2015-5936, CVE-2015-5937, CVE-2015-5939).
- Multiple out of bounds read issues existed in the NVIDIA graphics driver. These issues were addressed through improved bounds checking (CVE-2015-7019, CVE-2015-7020).
- Multiple vulnerabilities existed in PHP versions prior to 5.5.29 and 5.4.45. These were addressed by updating PHP to versions 5.5.29 and 5.4.45 (CVE-2015-0235, CVE-2015-0273, CVE-2015-6834, CVE-2015-6835, CVE-2015-6836, CVE-2015-6837, CVE-2015-6838).

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 bypassing 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.

RECOMMENDATIONS:

We recommend the following actions 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.

REFERENCES:

Apple:

<https://support.apple.com/en-us/ht201222>

CVE

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0273>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3565>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5916>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5924>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5924>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5925>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6992>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6993>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6994>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6995>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6996>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6997>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6999>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7000>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7002>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7003>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7004>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7006>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7007>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7008>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7009>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7010>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7011>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7012>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7013>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7014>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7015>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7016>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7017>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7018>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7019>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7020>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7021>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7022>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7023>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7035>