



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

July 01, 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:
SA2015-071**

**DATE ISSUED:
07/01/2015**

**SUBJECT:
Multiple Vulnerabilities in Apple Products Could Allow Remote Code Execution**

OVERVIEW:
Multiple vulnerabilities have been discovered in Apple iOS, Mac OS X, and Safari. Apple iOS is an operating system for iPhone, iPod touch, iPad, and Apple TV. 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 are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Apple Mac OS X Yosemite prior to 10.10.4
- Apple iOS prior to 8.4
- Apple Safari 6 Prior To 6.2.7
- Apple Safari 7 Prior To 7.1.7
- Apple Safari 8 Prior To 8.0.7

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 and 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:

- An information-disclosure vulnerability that affects the 'WebKit PDF' component. Specifically, the issue occurs when clicking a maliciously crafted link in a PDF embedded in a webpage (CVE-2015-3660).
- An information-disclosure vulnerability exists in the authorization checks for renaming WebSQL tables. Attackers can exploit this issue by enticing an unsuspecting user to view a specially crafted webpage to access databases belonging to other websites. [CVE-2015-3727]
- A security-bypass vulnerability exists where it would preserve the Origin request header for cross-origin redirects. Attackers can exploit this issue by enticing an unsuspecting user to view a specially crafted webpage to bypass CSRF protections. [CVE-2015-3658]
- An arbitrary code-execution vulnerability exists in SQLite authorizer which allowed invocation of arbitrary SQL functions. Attackers can exploit this issue by enticing an unsuspecting user to view a specially crafted webpage to execute arbitrary code-execution. [CVE-2015-3659]
- A remote memory-corruption vulnerability which may allow attackers to cause denial-of-service conditions (CVE 2015-3664, CVE 2015-3665, CVE 2015-3669)
- Attackers can exploit these issues to bypass security restrictions, to access sensitive information, to execute arbitrary code in the context of the currently logged-in user, to redirect attacker-controlled site.
- A privilege-escalation vulnerability affects the 'Admin Framework' component. Specifically, this issue occurs when checking XPC entitlements. An attacker can exploit this issue to gain admin privileges without properly authenticating (CVE-2015-3671).
- A privilege-escalation vulnerability affects the 'Admin Framework' component. Specifically, this issue occurs due to an error in the handling of user authentication (CVE-2015-3672).
- A local privilege-escalation vulnerability affects the 'Admin Framework' component. Specifically, this issue occurs due to an error in the Directory Utility. An attacker can exploit this issue by moving and modifying the Directory Utility to execute code within an entitled process and gain root privileges (CVE-2015-3673).
- A memory-corruption vulnerability affects the 'afpserver' component. Specifically, this issue exists in the AFP server. An attacker can exploit this issue to cause unexpected application termination or arbitrary code execution (CVE-2015-3674).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to an access security-bypass vulnerability affecting the 'apache' component. Specifically, this issue occurs because the default Apache configuration does not include 'mod_hfs_apple'. An attacker can exploit this issue to access some files in the directory using a specially crafted URL (CVE-2015-3675).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to an information-disclosure vulnerability affecting the 'AppleGraphicsControl' component. An attacker can exploit this issue to disclose the kernel memory layout using a specially-crafted application (CVE-2015-3676).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to an information-disclosure vulnerability affecting the 'AppleFSCompression' component. Specifically, this issue

exists in the LZVN compression. An attacker can exploit this issue to disclose the kernel memory layout using a specially-crafted application (CVE-2015-3677).

- Apple Mac OS X Yosemite prior to v10.10.4 is prone to a memory-corruption vulnerability affecting the 'AppleThunderboltEDMService' component. Specifically, this issue occurs due to an error in the handling of certain Thunderbolt commands from local processes. An attacker can exploit this issue to execute arbitrary code with system privileges using a specially-crafted application. (CVE-2015-3678).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to multiple memory-corruption vulnerabilities affect the 'ATS' component.
- Specifically, this issue occurs due to an error in the handling of certain fonts. An attacker can exploit these issues to cause unexpected application termination or arbitrary code execution using a specially-crafted font file (CVE-2015-3679, CVE-2015-3680, CVE-2015-3681, CVE-2015-3682).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to a memory-corruption vulnerability affecting the 'Bluetooth' component.
- Specifically, this issue occurs due to an error in the Bluetooth HCI interface. An attacker can exploit this issue to execute arbitrary code with system privileges using a specially-crafted application (CVE-2015-3683).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to an arbitrary code-execution vulnerability affecting the 'Display Drivers' component. Specifically, this issue occurs due to an error in the Monitor Control Command Set kernel extension. An attacker can exploit this issue to execute arbitrary code with system privileges using a specially-crafted application (CVE-2015-3691).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to an out-of-bounds write issue affecting the 'Display Drivers' component.
- Specifically, this issue occurs due to an error in the NVIDIA graphics driver. An attacker can exploit this issue to execute arbitrary code with system privileges using a specially-crafted application (CVE-2015-3712).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to multiple buffer-overflow vulnerabilities affect the 'Intel Graphics Driver' component. An attacker can exploit these issues to execute arbitrary code with system privileges (CVE-2015-3695, CVE-2015-3696, CVE-2015-3697, CVE-2015-3698, CVE-2015-3699, CVE-2015-3700, CVE-2015-3701, CVE-2015-3702).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to multiple memory-corruption vulnerabilities affect the 'IOAcceleratorFamily' component. An attacker can exploit these issues to execute arbitrary code with system privileges using a specially-crafted application (CVE-2015-3705, CVE-2015-3706).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to multiple remote code execution vulnerabilities affect the 'IOFireWireFamily' component. Specifically, these issues exist due to a null pointer dereference error. An attacker can exploit these issues to execute arbitrary code with system privileges using a specially-crafted application (CVE-2015-3707).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to an information-disclosure vulnerability affecting the 'Kernel' component. Specifically, this issue occurs due to an error in the handling of APIs related to kernel extensions. An attacker can exploit this issue to disclose the kernel memory layout using a specially-crafted application (CVE-2015-3720).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to multiple remote code execution vulnerabilities affect the 'Install Framework Legacy' component. Specifically, these issues exist due to the way Install.framework's 'runner' setuid binary dropped privileges. An attacker can exploit these issues to execute arbitrary code with system privileges using a specially-crafted application (CVE-2015-3704).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to a security-bypass vulnerability affecting the 'kext tools' component. Specifically, this issue occurs because kextd follows symbolic links while creating a new file. An attacker can exploit this issue to overwrite arbitrary files using a specially-crafted application (CVE-2015-3708).

- Apple Mac OS X Yosemite prior to v10.10.4 is prone to a local security-bypass vulnerability affecting the 'kext tools' component. Specifically, this issue occurs due to a time-of-check time-of-use (TOCTOU) race condition error when validating the paths of kernel extensions. A local attacker can exploit this issue to load unsigned kernel extensions (CVE-2015-3709).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to an information-disclosure vulnerability affecting the 'ntfs' component. An attacker can exploit this issue to disclose kernel memory content using a specially-crafted application (CVE-2015-3711).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to multiple memory-corruption vulnerabilities affecting the 'QuickTime' component. Specifically, these issues occur when processing a specially crafted 'movie' file. An attacker can exploit these issues to execute arbitrary code or terminate application (CVE-2015-3661, CVE-2015-3662, CVE-2015-3663, CVE-2015-3666, CVE-2015-3667, CVE-2015-3668, CVE-2015-3713).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to a security vulnerability affecting the 'Security' component. Specifically, this issue occurs because it fails to properly prevent tampered application from launching (CVE-2015-3714).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to a security-bypass vulnerability affecting the 'Security' component. Specifically, this issue occurs because the code signing fails to verify libraries loaded outside the application bundle. An attacker can exploit this issue to bypass code signing checks using a specially-crafted application (CVE-2015-3715).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to a command-injection vulnerability affecting the 'Spotlight' component. Specifically, this issue occurs when handling filenames of photos added to the local photo library. An attacker can exploit this issue by searching a specially-crafted file with Spotlight (CVE-2015-3716).
- Apple Mac OS X Yosemite prior to v10.10.4 is prone to a remote code execution vulnerability affecting the 'System Stats' component. Specifically, this issue occurs due to a type confusion error in systemstatsd's handling of interprocess communication. An attacker can exploit this issue to execute arbitrary code as the systemstatsd process using a specially-crafted application (CVE-2015-3718).
- A memory-corruption vulnerability that affects the 'CFNetwork HTTPAuthentication' component. Specifically, this issue exists in the handling of certain URL credentials (CVE-2015-3684).
- Multiple memory-corruption vulnerabilities that affect the 'CoreText' component. Specifically, these issues occur when processing text files. An attacker can exploit these issues by sending specially crafted text file (CVE-2015-1157, CVE-2015-3685, CVE-2015-3686, CVE-2015-3687, CVE-2015-3688, CVE-2015-3689).
- An information-disclosure vulnerability exists in the processing of disk images. An attacker can exploit this issue to determine kernel memory layout (CVE-2015-3690).
- A memory-corruption vulnerability that affects the 'FontParser' component. Specifically, this issue exists in the processing of font files (CVE-2015-3694).
- A memory-corruption vulnerability that affects the 'TrueTypeScaler' component. Specifically, this issue exists in the processing of font files (CVE-2015-3719).
- A memory-corruption vulnerability that affects the 'ImageIO' component. An attacker can exploit this issue by sending a specially crafted '.tiff' file (CVE-2015-3703).
- An information-disclosure vulnerability exists in the handling of HFS parameters. An attacker can exploit this issue to determine kernel memory layout (CVE-2015-3721).
- A security vulnerability that exists in the support for HTML email which allows message content to be refreshed with an arbitrary webpage. Specifically, this issue affects the 'Mail' component. An attacker can exploit this issue to replace the message content with an arbitrary webpage when the message is viewed through a crafted mail (CVE-2015-3710).
- Multiple buffer-overflow vulnerabilities because they fail to properly bounds-check user-supplied input before copying it to an insufficiently sized memory buffer. Specifically, these issues affect the 'SQLite' printf implementation (CVE-2015-3717).

- A security-bypass vulnerability exists in the installation logic for universal provisioning profile apps. Specifically, this issue affects the 'Application Store' component. An attacker can exploit this issue to allow collision with existing bundle IDs (CVE-2015-3722).
- Multiple memory corruption vulnerabilities exist in the handling of ICC profiles. Specifically, these issues affect the 'CoreGraphics' component. An attacker can exploit these issues by sending a specially crafted PDF file (CVE-2015-3723 and CVE-2015-3724).
- A security-bypass vulnerability exists in the installation logic for universal provisioning profile apps on the watch. Specifically, this issue affects the 'MobileInstallation' component. An attacker can exploit this issue to allow collision with existing bundle IDs (CVE-2015-3725).
- Multiple arbitrary-code execution vulnerabilities exist in the parsing of SIM/UIM payloads. Specifically, these issues affect the 'Telephony' component. An attacker can exploit these issues through crafted SIM cards (CVE-2015-3726).
- A security-bypass vulnerability exists in the WiFi manager's evaluation of known access point advertisements. Specifically, this issue affects the 'WiFi Connectivity' component. An attacker can exploit this issue to auto-associate with untrusted access points advertising a downgraded ESSID security type (CVE-2015-3728). 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:

We recommend the following actions be taken:

Upgrade to Apple Mac OS X Yosemite 10.10.4 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:

SecurityFocus

www.securityfocus.com/advisories/35714

www.securityfocus.com/advisories/35716

www.securityfocus.com/advisories/35717

www.securityfocus.com/advisories/35716

www.securityfocus.com/advisories/35715

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1157>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3658>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3659>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3660>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3661>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3662>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3663>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3664>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3665>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3666>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3726>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3727>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3728>