



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

**September 18, 2014**

*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:**

SA2014-059

**DATE(S) ISSUED:**

09/18/2014

**SUBJECT:**

Multiple Vulnerabilities in AppleiOS Prior to iOS 8 and TV Prior to TV 7

**OVERVIEW:**

Multiple vulnerabilities have been discovered in AppleiOS Prior to iOS 8 and TV Prior to TV 7. Apple iOS is an operating system for iPhone, iPod touch, and iPad. The iPhone is a mobile phone that runs on the ARM architecture. The iPod touch is a portable music player. The iPad is a tablet device. 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 AppleiOS.

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:** Updates are available.

**SYSTEMS AFFECTED:**

- AppleiOS Prior to iOS 8
- TV Prior to TV 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 vulnerabilities have been discovered in Apple iOS Prior to iOS 8 and TV Prior to TV 7. 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 Update 2014-003. The vulnerabilities are as follows:

- An information-disclosure vulnerability that occurs because of an error in the authentication with LEAP. An attacker can exploit this issue to obtain WiFi credentials. [CVE-2014-4364]
- An information-disclosure vulnerability occurs in the access control logic for accounts. Attacker can exploit this issue by using a sandboxed application to gain information about the currently-active iCloud account, including the name of the account. [CVE-2014-4423]
- A local security-bypass vulnerability because of a logic error in AssistiveTouch's handling of events, which results in the screen not locking. [CVE-2014-4368]
- A local information-disclosure vulnerability that occurs because an attacker with access to an iOS device may access sensitive user information from logs. [CVE-2014-4357]
- A local information-disclosure vulnerability that occurs because an attacker with physical access to the device may be able to read the address book. Specifically, this issue exists because the address book was encrypted with a key protected only by the hardware UID. [CVE-2014-4352]
- A local privilege-escalation vulnerability occurs due to a race condition in the App Installation. A local attacker with the privileges of writing to '/tmp' can exploit this issue to install an unverified app.[CVE-2014-4386]
- A local privilege-escalation vulnerability occurs due to a path traversal issue in the App Installation. A local attacker can exploit this issue to install an unverified app.[CVE-2014-4384]
- A spoofing vulnerability occurs due to a validation error exists in the handling of update check responses. [CVE-2014-4383]
- A security vulnerability occurs because Bluetooth is unexpectedly enabled by default after upgrading iOS. [CVE-2014-4354]
- An integer-overflow vulnerability affects the CoreGraphics component.
- Specifically, this issue occurs due to improper handling of PDF files. [CVE-2014-4377]
- A denial-of-service vulnerability due to an out-of-bound read error when handling PDF files. An attacker can exploit this issue to cause an unexpected application termination or an information disclosure. [CVE-2014-4378]
- An XML External Entity injection vulnerability due to an error in the 'NSXMLParser' when handling XML file. An attacker can exploit this issue to obtain potentially sensitive information. [CVE-2014-4374]
- A security-bypass vulnerability occurs because the API for determining the 'frontmost' app did not have sufficient access control. [CVE-2014-4361]
- A race-condition vulnerability exists in how attachments were deleted. Specifically, this issue occurs because attachments may persist after the parent iMessage or MMS is deleted. [CVE-2014-4353]
- A denial-of-service vulnerability due to a NULL-pointer dereference error when handling of 'IOAcceleratorFamily' API arguments. [CVE-2014-4369]
- A denial-of-service vulnerability due to a NULL-pointer dereference error in the 'IntelAccelerator' driver. [CVE-2014-4373]

- A denial-of-service vulnerability due to an out-of-bound read error when handling 'IOHIDFamily' function. An attacker can exploit this issue to bypass kernel address space layout randomization. [CVE-2014-4379]
- A heap-based buffer-overflow vulnerability exists in the IOHIDFamily's when handling key-mapping properties. An attacker can exploit this issue to execute arbitrary code with system privileges. [CVE-2014-4404]
- A denial-of-service vulnerability due to a NULL-pointer dereference error in the IOHIDFamily's when handling key-mapping properties. [CVE-2014-4405]
- An arbitrary-code-execution vulnerability due to an out-of-bound write error in the IOHIDFamily kernel extension. An attacker can exploit this issue to execute arbitrary code with kernel privileges. [CVE-2014-4380]
- A security-bypass vulnerability affects the random number generator. Specifically, this issue occurs because of insecure cryptography algorithm. An attacker can exploit this issue to bypass the hardening measures in kernel. [CVE-2014-4422]
- An arbitrary code-execution vulnerability affects the 'Libnotify' component. Specifically, this issue occurs due to out-of-bounds write issue. An attacker can exploit this issue to execute arbitrary code with root privileges by using malicious application. [CVE-2014-4381]
- An information-disclosure vulnerability affects the 'Mail' component. Specifically, this issue occurs because server sends the login credentials in plain text even if it has advertised the LOGINDISABLED IMAP capability. An attacker can exploit this issue to obtain login credentials in plain text. [CVE-2014-4366]
- A security vulnerability affects the 'Profiles' component. Specifically, this issue occurs when upgrading iOS. An attacker can exploit this issue to enable voice dial automatically. [CVE-2014-4367]
- An information-disclosure vulnerability affects the 'Safari' component. Specifically, this issue exists in the handling of saved passwords when autofilled. An attacker can exploit this issue to intercept user credentials. [CVE-2014-4363]
- An information-disclosure vulnerability affects the 'Sandbox Profiles' component. Specifically, this issue exists in the handling of third-party app sandbox. An attacker can exploit this issue to obtain Apple ID information. [CVE-2014-4362]
- A information-disclosure vulnerability affects the 'Settings' component. Specifically, this issue occurs when previewing of text message notifications at the lock screen. An attacker can exploit this obtain the contents of received messages even when previews were disabled in Settings. [CVE-2014-4356]
- A local security-bypass vulnerability issue exists in the 'syslog' component. An attacker can exploit this issue to change permissions on arbitrary files through symbolic link attack. [CVE-2014-4372]
- A security-bypass vulnerability affects the 'WebKit' component. Specifically, this issue occurs when private browsing. An attacker can exploit this issue to track users even when private browsing is enabled. [CVE-2014-4409]
- An information disclosure vulnerability exists in the handling of 'IOKit' functions. Specifically, this issue affects the 'IOKit' component. [CVE-2014-4407]
- A remote code-execution vulnerability exists in the handling of certain metadata fields of 'IODataQueue' objects due to an error in the validation. Specifically, this issue affects the 'IOKit' component. [CVE-2014-4418]
- A remote code-execution vulnerability exists in the handling of certain metadata fields of 'IODataQueue' objects due to an error in the validation. Specifically, this issue affects the 'IOKit' component. [CVE-2014-4388]
- An integer buffer-overflow vulnerability exists in the handling of 'IOKit' functions. Specifically, this issue affects the 'IOKit' component. [CVE-2014-4389]
- Multiple unspecified security vulnerabilities exist. Specifically, these issues affect the 'Kernel' component. [CVE-2014-4371, CVE-2014-4419, CVE-2014-4420, and CVE-2014-4421]
- A double-free issue exists in the handling of Mach ports. Specifically, this issue affects the 'Kernel' component. [CVE-2014-4375]

- An out-of-bounds read issue exists in the 'rt\_setgate'. Specifically, this issue affects the 'Kernel' component. [CVE-2014-4408]

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:**

We recommend the following actions be taken:

- Update vulnerable Apple products 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 visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or un-trusted sources.

#### **REFERENCES:**

##### **Apple:**

<http://www.apple.com/iphone/softwareupdate>

##### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4352>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4353>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4354>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4356>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4357>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4361>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4362>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4363>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4364>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4366>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4367>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4368>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4369>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4371>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4372>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4373>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4374>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4375>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4377>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4378>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4379>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4380>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4381>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4383>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4384>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4386>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4388>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4389>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4404>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4405>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4407>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4408>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4409>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4418>

<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-2014-4422>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4423>

**SecurityFocus:**

<http://www.securityfocus.com/bid/69882>  
<http://www.securityfocus.com/advisories/33426>  
<http://www.securityfocus.com/advisories/33427>