

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 ISSUED:

01/28/2015

SUBJECT:

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

OVERVIEW:

Multiple vulnerabilities have been discovered in Apple iOS Prior to iOS 8 and TV Prior to TV 7. Apple iOS is an operating system for iPhone, iPod touch, iPad and Apple TV. 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. Apple TV is a media streaming appliance.

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 Apple iOS.

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:

- Apple iOS Prior to iOS 8.1.3
- Apple TV Prior to TV 7.0.3

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 8.1.3 and TV Prior to TV 7.0.3. 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 Updates 2015-000 and 2015-001. The vulnerabilities are as follows:

- A maliciously crafted afc command may allow access to protected parts of the filesystem [CVE-2014-4480]
- Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution [CVE-2014-4481]
- A local user may be able to execute unsigned code [CVE-2014-4455]
- Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution [CVE-2014-4483]
- Processing a maliciously crafted .dfont file may lead to an unexpected application termination or arbitrary code execution [CVE-2014-4484]
- Viewing a maliciously crafted XML file may lead to an unexpected application termination or arbitrary code execution [CVE-2014-4485]
- A malicious application may be able to execute arbitrary code with system privileges [CVE-2014-4486], [CVE-2014-4487], [CVE-2014-4488], [CVE-2014-4489], and [CVE-2014-4495]
- A website may be able to bypass sandbox restrictions using the iTunes Store [CVE-2014-8840]
- Maliciously crafted or compromised iOS applications may be able to determine addresses in the kernel [CVE-2014-4491] and [CVE-2014-4496]
- A malicious, sandboxed app can compromise the networkd daemon [CVE-2014-4492]
- A malicious enterprise-signed application may be able to take control of the local container for applications already on a device [CVE-2014-4493]
- Enterprise-signed applications may be launched without prompting for trust [CVE-2014-4494]
- Visiting a website that frames malicious content may lead to UI spoofing [CVE-2014-4467]
- Style sheets are loaded cross-origin which may allow for data exfiltration [CVE-2014-4465]
- Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution [CVE-2014-3192], [CVE-2014-4459], [CVE-2014-4466], [CVE-2014-4468], [CVE-2014-4469], [CVE-2014-4470], [CVE-2014-4471], [CVE-2014-4472], [CVE-2014-4473], [CVE-2014-4474], [CVE-2014-4475], [CVE-2014-4476], [CVE-2014-4477], and [CVE-2014-4479]

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:

The following actions should 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://lists.apple.com/archives/security-announce/2015/Jan/msg00000.html>
<http://lists.apple.com/archives/security-announce/2015/Jan/msg00001.html>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3192>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4455>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4459>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4465>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4466>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4467>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4468>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4469>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4470>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4471>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4472>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4473>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4474>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4475>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4476>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4477>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4479>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4480>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4481>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4483>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4484>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4485>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4486>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4487>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4488>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4489>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4491>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4492>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4493>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4494>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4495>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8840>

SecurityFocus:

<http://www.securityfocus.com/advisories/34710>
<http://www.securityfocus.com/advisories/34711>
<http://www.securityfocus.com/bid/72327>
<http://www.securityfocus.com/bid/72333>
<http://www.securityfocus.com/bid/72334>

TLP:WHITE

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

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