

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:

01/20/2016

SUBJECT:

Multiple Vulnerabilities in Apple Products Could Allow Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in OS X, Safari, and iOS. 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. 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, arbitrary code execution within the context of the application, or the bypassing of security restrictions. 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 10.11.3
- Safari prior to 9.0.3
- iOS prior to 9.2.1

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 vulnerabilities have been discovered in OS X, Safari, and iOS. The most serious of these vulnerabilities could lead to arbitrary code execution. Details of all vulnerabilities are as follows:

- A type confusion issue existed in libxslt. This issue was addressed through improved memory handling. (CVE-2015-7995)

- A memory corruption issue existed in AppleGraphicsPowerManagement. This issue was addressed through improved memory handling. (CVE-2016-1716)
- A memory corruption issue existed in the parsing of disk images. This issue was addressed through improved memory handling. (CVE-2016-1717)
- A memory corruption issue existed in IOAcceleratorFamily. This issue was addressed through improved memory handling. (CVE-2016-1718)
- A memory corruption issue existed in IOHIDFamily API. This issue was addressed through improved memory handling. (CVE-2016-1719)
- A memory corruption issue existed in IOKit. This issue was addressed through improved memory handling. (CVE-2016-1720)
- A memory corruption issue existed in the kernel. This was addressed through improved memory handling. (CVE-2016-1721)
- A memory corruption issue existed in syslog. This was addressed through improved memory handling. (CVE-2016-1722)
- Multiple memory corruption issues existed in WebKit. These issues were addressed through improved memory handling. (CVE-2016-1723, CVE-2016-1724, CVE-2016-1725, CVE-2016-1726, CVE-2016-1727)
- A privacy issue existed in the handling of the "a:visited button" CSS selector when evaluating the containing element's height. This was addressed through improved validation. (CVE-2016-1728)
- An issue existed when searching for scripting libraries. This issue was addressed through improved search order and quarantine checks. (CVE-2016-1729)

An issue existed that allowed some captive portals to read or write cookies. The issue was addressed through an isolated cookie store for all captive portals. (CVE-2016-1730)

Successful exploitation could result in an attacker gaining the same privileges as the logged on user, arbitrary 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/en-us/HT205730>

<https://support.apple.com/en-us/HT205731>

<https://support.apple.com/en-us/HT205732>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7995>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1716>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1717>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1718>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1719>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1720>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1721>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1722>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1723>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1724>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1725>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1726>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1727>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1728>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1729>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1730>

TLP: WHITE

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

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