

*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:**

09/13/2016

**SUBJECT:**

Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in iOS, watchOS, and Xcode, the most severe of which could result in arbitrary code execution. Apple iOS is an operating system for iPhone, iPod touch, and iPad. watchOS is the mobile operating system of the Apple Watch. Xcode is a development platform used to make apps on Apple products. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code, bypass certain security measures or lead to information disclosure.

**THREAT INTELLIGENCE:**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- iOS prior to version 10.01 for iPhone 5 and later, iPod touch (6th generation) and later, and iPad 4 and later
- watchOS prior to 3 for Apple Watch Sport, Apple Watch, Apple Watch Edition, and Apple Watch Hermes
- Xcode prior to version 8 for OS X El Capitan v10.11.5 and later

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **Medium**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **Medium**

**Home users: Low**

**TECHNICAL SUMMARY:**

Apple has released patches for multiple vulnerabilities that have been discovered in Apple products. The most severe of these vulnerabilities could result in arbitrary code execution. Details of these vulnerabilities are as follows:

- An issue existed in iOS updates, which did not properly secure user communications (CVE-2016-4741)
- A permissions issue existed in PlaceData (CVE-216-4719)

- The iOS keyboard was inadvertently caching sensitive information (CVE-2016-4746)
- An issue existed when handling untrusted certificates (CVE-2016-4747)
- An issue existed when using Handoff for Messages (CVE-2016-4740)
- An issue existed in AirPrint preview (CVE-2016-4749)
- An access control issue existed in SMS draft directories (CVE-2016-4620)
- Multiple memory corruption issues in Xcode that could cause unexpected application termination or arbitrary code execution were addressed through improved memory handling (CVE-2016-4704, CVE-2016-4705)

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code, bypass certain security measures, or lead to information disclosure.

#### **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/HT207143>  
<https://support.apple.com/en-us/HT207140>  
<https://support.apple.com/en-us/HT207141>  
<https://support.apple.com/kb/HT207145>

##### **CVE**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4620>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4704>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4705>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4719>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4740>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4741>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4746>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4747>  
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4749>

**TLP: WHITE**

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

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