

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:

06/19/2015

SUBJECT:

Cross App Resource Access Vulnerability in Apple Operating Systems Could Allow Information Disclosure

OVERVIEW:

A Cross App Resource Access vulnerability has been discovered in Apple Mac OS X and Apple iOS. Mac OS X is an operating system for Apple computers. Apple iOS is an operating system for iPhone, iPod touch, iPad, Apple TV. This vulnerability can be exploited if a user downloads a malicious application onto their system or device.

Successful exploitation could result in an attacker gaining access to sensitive information on the device including passwords, documents, or photos stored on the device or by other applications.

THREAT INTELLIGENCE:

A full report detailing the vulnerability has been published. At this time there are no reports of this vulnerability being used in the wild.

SYSTEMS AFFECTED:

- Apple Mac OS X prior to version 10.10.3
- Apple iOS prior to version 8.3

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:

A Cross App Resource Access vulnerability has been discovered in OSX and iOS, due to a failure to treat other applications on the device as untrusted. An attacker can craft a malicious application and submit it to the app store as a legitimate application. Once approved, the attacker can entice a victim to download the application, allowing access to data stored on the system as well as data stored by other applications. Based on a sampling of the top 1,612 OSX applications and 200 iOS applications at the time, the researchers reported a vulnerability rate of 88.6% across the App Stores.

Successful exploitation could result in an attacker gaining access to sensitive information including the OSX system keychain, iCloud secret token, passwords, and any other data stored or processed by a vulnerable application.

RECOMMENDATIONS:

The following actions should be taken:

- Once a patch is released from Apple perform updates immediately after appropriate testing.
- Remind users not to download applications from un-trusted or unknown sources.

REFERENCES:

Krebs On Security:

<http://krebsonsecurity.com/2015/06/critical-flaws-in-apple-samsung-devices/>

Original Report:

<https://drive.google.com/file/d/0BxxXk1d3yyuZOFIsdkNMSGswSGs/view>

TLP: WHITE

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

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