

*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:**

08/25/2016

**SUBJECT:**

Multiple Vulnerabilities in Apple Products Could Allow For Arbitrary Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in iOS, the most severe of which could allow for arbitrary code execution. Apple iOS is an operating system for iPhone, iPod touch, and iPad. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code with kernel privileges.

**THREAT INTELLIGENCE:**

These vulnerabilities are associated with three zero-days (nicknamed "Trident") and a tool called "Pegasus." These vulnerabilities have been publicly disclosed and a tool exists to perform the exploit. There are reports of the vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- iOS prior to 9.3.5 for iPhone 4s and later, iPod touch (5th generation) and later, and iPad 2 and later

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government: **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. These vulnerabilities can be exploited by convincing a user to visit a specially crafted webpage. The most severe of these vulnerabilities could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A vulnerability exists in the kernel that may lead to disclosure of the kernel's location in memory (CVE-2016-4655).

- A vulnerability exists in the kernel that may lead to memory corruption and covert jailbreaking of the device (CVE-2016-4656).
- A vulnerability exists in Webkit, allowing for memory corruption (CVE-2016-4657).

**RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by [Apple](#) to vulnerable systems immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from untrusted sources.

**REFERENCES:****Apple:**

<https://support.apple.com/en-us/HT207107>

**Lookout:**

<https://blog.lookout.com/blog/2016/08/25/trident-pegasus/>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4655>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4656>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4657>

**TLP: WHITE**

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

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