

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:

09/02/2016

SUBJECT:

Multiple Vulnerabilities in Apple Products Could Allow For Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Apple OS X and Safari, the most severe of which could allow for arbitrary code execution. Apple OS X is the operating system utilized by Macintosh computers. Apple Safari is a web browser available for OS X, iOS and Microsoft Windows. Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code with kernel privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

THREAT INTELLIGENCE:

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

SYSTEM AFFECTED:

- OS X Yosemite prior to version 10.10.5
- OS X El Capitan prior to version 10.11.6
- OS X Mavericks prior to version 10.9.5
- Apple Safari prior to version 9.1.3

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 previously discovered vulnerabilities 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 that may lead to memory corruption and arbitrary code execution (CVE-2016-4654).
- A vulnerability exists that may lead to disclosure of the kernel's location in memory (CVE-2016-4655).
- A vulnerability exists that may lead to memory corruption and execution of arbitrary code with kernel privileges (CVE-2016-4656)

Successful exploitation of the most severe of these vulnerabilities could allow an attacker to execute arbitrary code with kernel privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full system rights.

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/HT207130>

<https://support.apple.com/en-us/HT207131>

Lookout:

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

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4654>

<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>

TLP: WHITE

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

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