

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:

08/05/2015

SUBJECT:

Vulnerability in Apple's OS X Could Allow for Privilege Escalation

OVERVIEW:

A vulnerability has been discovered in Apple's OS X, which could allow for privilege escalation. Apple's OS X is an operating system for Apple computers. Successful exploitation of this vulnerability could allow an attacker to open, create, or modify files with root privileges which could result in the installation of malware or other unwanted programs, or the execution of arbitrary code.

THREAT INTELLIGENCE

There are reports of this vulnerability being exploited in the wild.

SYSTEM AFFECTED:

- Apple's OS X version 10.10.4 and prior

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 vulnerability has been discovered in Apple's OS X, which could allow for privilege escalation. The vulnerability exists in how the operating system handles the dyld dynamic linker and the DYLD_PRINT_TO_FILE environment variable. This vulnerability could allow for any file on the system to be opened or modified with root-like privileges. One such example could allow for the sudoers file to be modified to allow shell commands to be executed with root privileges without the need for a sudo password.

Successful exploitation of this vulnerability could allow an attacker to open, create, or modify files with root privileges which could result in the installation of malware or other unwanted programs, or the execution of arbitrary code.

RECOMMENDATIONS:

The following actions should be taken:

- Once a fix is released by Apple, update immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments, especially those from un-trusted sources.

REFERENCES:

Ars Technica:

<http://arstechnica.com/security/2015/08/0-day-bug-in-fully-patched-os-x-comes-under-active-exploit-to-hijack-macs/>

ZDNet:

<http://www.zdnet.com/article/researcher-unveils-new-privilege-vulnerability-in-apples-mac-os-x/>
<http://www.zdnet.com/article/apple-mac-zero-day-flaw-hands-over-root-access-without-system-passwords/>

TLP: WHITE

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

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