

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.

DATE(S) ISSUED:

10/29/2014

SUBJECT:

Multiple Vulnerabilities in Apple MAC OSX prior to 10.9.5 and Apple QuickTime prior to 7.7.6

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Apple MAC OSX prior to 10.9.5 and Apple QuickTime prior to 7.7.6. Mac OS X is an operating system for Apple computers. Apple QuickTime Player is used to play media files on Microsoft Windows and Mac OS X operating systems. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage, or opens a specially crafted file, including an email attachment, using a vulnerable version of OS X or QuickTime.

Successful exploitation could result in an attacker gaining the same privileges as the logged on user, remote code execution within the context of the application, and bypass of security systems. Failed attacks may cause a Denial of Service condition within the targeted delivery method. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

At this time, there is no known proof-of-concept code available.

SYSTEM AFFECTED:

- Apple Mac OS X versions before 10.9.5
- Apple QuickTime versions before 7.7.6

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:

Multiple remote code execution vulnerabilities have been discovered in Apple MAC OS X and Apple QuickTime that could allow remote code execution. These vulnerabilities can be exploited if a user visits or is redirected to a specially crafted webpage or opens a specially crafted file. Details of these vulnerabilities are as follows:

- Apple Mac OS X is prone to a memory-corruption vulnerability because it fails to perform adequate bounds checks on user-supplied input. [CVE-2014-1391]
- Apple QuickTime is prone to a heap-memory-corruption vulnerability because it fails to properly handle specially crafted versions and flags. [CVE-2014-4979]
- Apple Mac OS X is prone to a remote buffer-overflow vulnerability that affects the 'QuickTime' component. Specifically, this issue occurs because it fails to properly handle a specially crafted 'm4a' file. [CVE-2014-4351]

Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

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 (one without administrative privileges) 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:

ZeroDay Initiative:

<http://www.zerodayinitiative.com/advisories/ZDI-14-264/>

<http://www.zerodayinitiative.com/advisories/ZDI-14-325/>

Apple:

<http://support.apple.com/kb/HT6443>

<http://support.apple.com/kb/HT6493>

<https://support.apple.com/kb/HT6535>

Security Focus:

<http://www.securityfocus.com/advisories/33431>

<http://www.securityfocus.com/advisories/33748>

<http://www.securityfocus.com/advisories/33801>

<http://www.securityfocus.com/bid/68852>

<http://www.securityfocus.com/bid/69907>

<http://www.securityfocus.com/bid/70643>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1391>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4351>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4979>