

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:

3/31/2010

SUBJECT:

Multiple Vulnerabilities in Apple QuickTime Player Could Allow for Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Apple QuickTime Player. QuickTime Player is used to play multimedia files on Microsoft Windows and Mac OS X operating systems. These vulnerabilities can be exploited if a user visits a malicious webpage or opens a malicious file, including an e-mail attachment, using a vulnerable version of QuickTime Player. Successful exploitation may 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.

SYSTEMS AFFECTED:

Apple QuickTime Player versions prior to 7.6.6

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

DESCRIPTION:

Multiple vulnerabilities have been discovered in Apple QuickTime Player. QuickTime Player is a media player for the Microsoft Windows and Mac OS X operating systems. Details of these vulnerabilities are as follows:

Two Integer Overflow Vulnerabilities

Two integer overflow vulnerabilities exist in QuickTime Player when handling malformed PICT images or FlashPix files. Viewing a maliciously crafted FlashPix movie file or PICT image may lead to an unexpected application termination or arbitrary code execution.

Six Memory Corruption Vulnerabilities

Six memory corruption vulnerabilities exist in QuickTime Player when handling malformed BMP images, color tables in movie files, malformed QDM2 and QDMC encoded audio content or malformed H.264 and Sorenson encoded movie files. Viewing a maliciously crafted movie, audio or image file may lead to an unexpected application termination or arbitrary code execution.

Eight Heap Buffer Overflow Vulnerabilities

Eight heap buffer overflow vulnerabilities exist in QuickTime Player when handling malformed PICT images or H.263, M-JPEG, FLC and RLE encoded movie files. Opening a maliciously crafted PICT

image or specially crafted movie files may lead to an unexpected application termination or arbitrary code execution.

These vulnerabilities can be exploited if a user has a vulnerable version of QuickTime Player and visits a malicious webpage or opens a malicious file, including an e-mail attachment. Successful exploitation may 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. Failed exploit attempts may result in denial-of-service conditions

RECOMMENDATIONS:

The following actions should be taken:

- Apply the appropriate updates to vulnerable systems immediately after appropriate testing. The update is available at: <http://www.apple.com/quicktime/download/>
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Consider removing the file association of the affected multimedia file types from Apple QuickTime Player.
- Do not visit unknown or un-trusted Web sites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments from unknown or un-trusted sources.

REFERENCES:

Apple:

<http://support.apple.com/kb/HT4104>

Security Focus:

<http://www.securityfocus.com/bid/39087>

Secunia:

<http://secunia.com/advisories/39133>

Vupen:

<http://www.vupen.com/english/advisories/2010/0746>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2837>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0059>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0060>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0062>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0514>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0515>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0516>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0517>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0518>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0519>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0520>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0526>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0527>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0528>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0529>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0536>