

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:

08/04/2011

SUBJECT:

Multiple Vulnerabilities in Apple QuickTime Player Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Apple QuickTime Player that could allow remote code execution. 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 Apple QuickTime Player. Successful exploitation will 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 7.6.9 and earlier

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 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, including an email attachment, with a vulnerable version of Apple QuickTime Player.

Apple has identified the following vulnerabilities:

- A buffer overflow vulnerability exists in the way Apple QuickTime Player handles specially crafted PICT image files.
- Multiple memory corruption vulnerabilities exist in QuickTime's handling of JPEG2000 images.
- A cross-origin issue exists in the way QuickTime plug-ins handle cross-site redirects. Visiting a maliciously crafted website may lead to the disclosure of video data from another site.
- An integer overflow exists in QuickTime's handling of RIFF WAV files.
- A memory corruption issue exists in QuickTime's handling of sample tables in QuickTime movie files.
- An integer overflow exists in QuickTime's handling of audio channels in movie files.
- A buffer overflow exists in QuickTime's handling of JPEG files.
- A heap buffer overflow exists in QuickTime's handling of GIF images.
- Multiple stack buffer overflows exist in the handling of H.264 encoded movie files.
- A stack buffer overflow exists in the QuickTime ActiveX control's handling of QTL (QuickTime Link) files. A QTL file is a text file that contains a link to a QuickTime movie, and is often found in web page hyperlinks.
- A heap buffer overflow exists in the handling of STSC atoms, STSS atoms, STSZ atoms, or STTS atoms in QuickTime movie files. Atoms are chunks of data that comprise a QuickTime movie file.

Successful exploitation of these vulnerabilities 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. Failed attempts could result in a denial-of-service.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Apple to vulnerable systems immediately after appropriate testing.
- Remind users not to download or open files from un-trusted websites.
- Remind users not to open e-mail attachments from unknown users or suspicious e-mails from trusted sources.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Apple:

<http://lists.apple.com/archives/security-announce/2011/Aug/msg00000.html>

SecurityFocus:

<http://www.securityfocus.com/advisories/22624>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0186>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0187>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0209>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0210>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0211>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0213>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0245>

<http://cve.mitre.org/cgi-bin/cvename.cgi?namehttp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0246>

<http://cve.mitre.org/cgi-bin/cvename.cgi?namehttp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0247>

<http://cve.mitre.org/cgi-bin/cvename.cgi?namehttp://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0248>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=%20CVE-2011-0249http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0249>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=%20CVE-2011-0250http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0250>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=%20CVE-2011-0251http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0251>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=%20CVE-2011-0252http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0252>