

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:

5/16/2012

SUBJECT:

Multiple Vulnerabilities in Apple QuickTime Could Allow Remote Code Execution

OVERVIEW:

Multiple vulnerabilities have been discovered in Apple QuickTime 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 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.

SYSTEMS AFFECTED:

Apple QuickTime versions prior to 7.7.2 for Windows and Mac OS X

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 versions prior to 7.7.2 for the Microsoft Windows and Mac OS X operating systems 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.

The details of these vulnerabilities are as follows:

- Multiple unspecified stack overflow vulnerabilities exist in the handling of TeXML files. To exploit these issues, an attacker creates a specially crafted website and entices users to visit the site. When the site is visited, the exploit is triggered resulting in remote code execution. (CVE-2012-0663)
- An unspecified heap overflow vulnerability exists in the application's handling of text tracks and H.264 encoded movie files. To exploit these issues, an attacker creates a specially crafted movie file and distributes that file to unsuspecting users. When the file is opened the exploit is triggered resulting in remote code execution.(CVE-2012-0664) (CVE-2012-0665)
- An unspecified stack buffer overflow vulnerability exists in the QuickTime plugin's handling of QTMovie objects. To exploit this issue, an attacker creates a specially crafted website and

entices users to visit the site. When the site is visited the exploit is triggered resulting in remote code execution. (CVE-2012-0666)

- A signedness issue exists in the handling of QTVR movie files. To exploit this issue, an attacker creates a specially crafted movie file and distributes that file to unsuspecting users. When the file is opened the exploit is triggered resulting in remote code execution. (CVE-2012-0667)
- Multiple unspecified buffer overflow vulnerabilities exist in the handling of RLE and Sorenson encoded movie files. To exploit this issue, an attacker creates a specially crafted movie file and distributes that file to unsuspecting users. When the file is opened the exploit is triggered resulting in remote code execution. (CVE-2012-0668) (CVE-2012-0669)
- An unspecified integer overflow vulnerability exists in QuickTime's handling of sean atoms. To exploit this issue, an attacker creates a specially crafted movie file and distributes that file to unsuspecting users. When the file is opened the exploit is triggered resulting in remote code execution. (CVE-2012-0670)
- An unspecified memory corruption vulnerability exists in the handling of “.pict” files. To exploit this issue, an attacker creates a specially crafted movie file and distributes that file to unsuspecting users. When the file is opened the exploit is triggered resulting in remote code execution. (CVE-2012-0671)
- An unspecified stack buffer overflow vulnerability exists in QuickTime's handling of file paths. The details of how this vulnerability can be exploited are currently unavailable. However, successful exploitation will result in remote code execution (CVE-2012-0265)
- For Mac OS X v10.6 systems, these issues are addressed in Security Update 2012-001 (MS-ISAC Advisory 2012-006) and 2012-002 (MS-ISAC Advisory 2012-034). For OS X Lion systems, these issues are addressed in OS X Lion v10.7.3 and v10.7.4.

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.

The following actions should be taken:

Apply appropriate patches provided by Apple to affected 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 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.

REFERENCES:

Apple:

<http://support.apple.com/kb/HT5261>

Security Focus:

<http://www.securityfocus.com/bid/53547>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0663>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0664>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0665>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0666>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0667>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0668>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0669>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0670>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0671>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0265>