

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:

8/17/2010

SUBJECT:

Vulnerability in Apple QuickTime Player Could Allow for Remote Code Execution

OVERVIEW:

A vulnerability has 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. This vulnerability 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 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:

QuickTime 7.6.6 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:

A vulnerability has been discovered in Apple QuickTime Player that could allow remote code execution. This vulnerability exists in the way the 'QuickTimeStreaming.qtx' library constructs a string to write to a debug log file. More specifically, this issue arises because Apple QuickTime Player does not perform sufficient boundary checks when parsing Synchronized Multimedia Integration Language (SMIL) file types containing overly long URL's.

This vulnerability can be exploited via an email attachment or through the web. In the email based scenario, the user would have to open the specially crafted Apple QuickTime file as an email attachment. In the web based scenario, a user would have to open a specially crafted Apple QuickTime file that is hosted on a website. Successful exploitation of this vulnerability 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 exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches 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.
- Consider removing the file association of the affected multimedia file types from Apple QuickTime Player.
- Consider blocking SMIL files at the network perimeter.
- 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://lists.apple.com/archives/security-announce/2010/aug/msg00002.html>

Security Focus:

<http://www.securityfocus.com/advisories/20244>

<http://www.securityfocus.com/bid/41962>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1799>