

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:

8/30/2010

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 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.

Exploit code is publicly available. There is currently no patch available for this vulnerability.

SYSTEMS AFFECTED:

- Apple QuickTime Player 7.6.7 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 issue affects the '_Marshaled_pUnk' backdoor method of the 'QTPlugin.ocx' ActiveX control. ActiveX controls are used to create distributed applications that work over the Internet through web browsers, typically using Microsoft's Internet Explorer.

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 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. Failed exploit attempts may result in a denial-of-service condition.

Exploit code is publicly available. There is currently no patch available for this vulnerability.

RECOMMENDATIONS:

The following actions should be taken:

- Install the appropriate vendor patch as soon as it becomes available after appropriate testing.
- Disable Active Scripting in Internet Explorer. For additional information on this please review the following [Microsoft Knowledge Base article](#).
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Consider removing Apple Quick Time Player file associations so that Apple Quick Time Player is not automatically launched when associated file types are opened.
- 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:**The Register:**

http://www.theregister.co.uk/2010/08/30/apple_quicktime_critical_vuln/

Ruben Santamarta:

http://reversemode.com/index.php?option=com_content&task=view&id=69&Itemid=1