I

Published on 09/21/08

Intego today announced that it has discovered a QuickTime bug which may be used as a vector for attack. Apple's QuickTime, the media software used to play music and movies on Mac OS X and Windows, has recently been update to version 7.5.5, but a serious bug has already been discovered that may be used as a vector for malicious attacks. Intego's Virus Monitoring Center is keeping a close eye on this bug and whether malicious users are attempting to add payload to QuickTime files.

Intego, the Macintosh security specialist, today announced that it has discovered a QuickTime bug which may be used as a vector for attack. Apple's QuickTime, the media software used to play music and movies on Mac OS X and Windows, has recently been update to version 7.5.5, but a serious bug has already been discovered that may be used as a vector for malicious attacks.

Exploit: OSX.Exploit.QT755-1
Discovered: September 18, 2008
Risk: Low

The "<? quicktime type= ?>" tag fails to handle long strings, which can lead to a heap overflow in QuickTime Player, iTunes, or any other program that attempts to display media using a QuickTime plug-in. This can be a browser, such as Apple's Safari, Microsoft Internet Explorer or Mozilla Firefox, or, on Mac OS X, could be any program that displays graphics or movies inline, such as Mail, or even the Finder if a user tries to view a file with Quick Look. For now, files which contain offending strings will crash programs attempting to display them, but malicious code could be added to such files, and may be executed with no user interaction, other than an attempt to view a file.

This bug can be remote or local, as QuickTime parses any supplied file for a recognized header even if the header does not correspond to the file type; for example, a malicious user could put XML content in an MP4 or MOV file, or could add a QuickTime media file to a web page which could then cause a browser to crash while executing malicious code.

Intego's Virus Monitoring Center is keeping a close eye on this bug and whether malicious users are attempting to add payload to QuickTime files. Intego will naturally update the virus definitions for Intego VirusBarrier X5 if this occurs. Intego will be posting more information, as it becomes available, on the Intego Mac Security Blog.

Intego:
http://www.intego.com

Intego develops and sells desktop Internet security and privacy software for Macintosh. Intego provides the widest range of software to protect users and their Macs from the dangers of the Internet. Intego's multilingual software and support repeatedly receives awards from Mac magazines, and protects more than one million users in over 60 countries. Intego has headquarters in the USA, France and Japan. For further information, please visit their website.

###

Rosaline Mills
PR Consultant

+44 (0)845 2577115

rosaline@bamboopr.co.uk

****
Link To Article: https://prmac.com/release-id-2858.htm
****