

27 November 2007

By: Victor Mihailescu, Apple News Editor



## [QuickTime Vulnerability Also Present in Os X Version](#)

*But only causes a Denial Of Service...*

Last week, there was a lot of stink made over by another QuickTime vulnerability for Windows. There have been quite a few of these vulnerabilities in Apple's software, but they have typically affected both Windows and OS X. So, it should not be surprising that the same issue was discovered on the Mac. Symantec's security response team dug a little deeper, and found that the Real-Time Streaming Protocol (RTSP) bug in QuickTime is also quite present in the Mac version of Apple media player. Although the vulnerability is in the same place as on the Windows version, it will behave differently on a Mac, and the Windows specific attack code fails to give a hacker access to OS X, instead causing QuickTime to crash. "We tested it, and the exploit does cause a denial of service," said Marc Fossi, manager of the Symantec team. Although the vulnerability is less severe than it is on Windows, Fossi warned that Mac users might not be in the clear, yet. "QuickTime vulnerabilities have tended to affect both Windows and Mac OS X, and it's always possible that a denial of service could lead to remote code execution." The security researcher also noted that, on Windows, Microsoft Internet Explorer Versions 6 and 7, as well as Apple's own browser, will further serve as a buffer, offering some additional protection against the attacks that are based on fooling users into visiting malicious or compromised sites hosting rigged streaming content. "The buffer overflow protection built into IE and in Safari prevents the exploit shell code from executing in the plug-in," said Fossi. Thus, in order to successfully attack users that are currently using these browsers, the current exploit would have to be further refined. It is important to note that users of Firefox, a very popular browser on the Windows platform, have no such buffer that they can rely on, and would be directly affected by the exploit as it is now.