

8 April 2008

By: Marius Oiaga, Technology News Editor



[Apple Adopts Windows Vista Security Mitigations](#)

For its own solutions

In a new move designed to add anti-hacking features to its solutions, Apple is contradicting the general perspective that its products offer [security by default](#), in contrast with Microsoft's software. The Cupertino-based hardware company is working to bulletproof its own software against hacking attempts and, in this context, managed to embrace security mitigations introduced as defaults into Windows Vista. The targeted product for the new exploit prevention mechanisms is none other than the QuickTime media player. Microsoft solutions, from the Windows operating systems to the Internet Explorer browsers, are generally perceived as inferior in terms of security to what Apple has to offer. And the Cupertino-based company has fueled this perspective through marketing. Still, Apple failed to hesitate in embracing security mitigations specific of the Windows Vista platform for QuickTime 7.4.5. According to [EWeek](#), citing sources familiar with the situation, Apple has integrated an exploit prevention mechanism (XPMs) into QuickTime 7.4.5 for [both Mac OS X and Windows](#). This was done via a recent update for the media player which also contributed to patching approximately a dozen of security vulnerabilities in the product. As far as QuickTime for Vista is concerned, the media player now comes with Address space layout randomization (ASLR). "ASLR moves images into random locations when a system boots and thus makes it harder for shell code to operate successfully. For a component to support ASLR, all components that it loads must also support ASLR. For example, if A.EXE consumes B.DLL and C.DLL, all three must support ASLR. By default, Windows Vista will randomize system DLLs and EXEs, but DLLs and EXEs created by ISVs must opt in to support ASLR," reads Microsoft's official description of the security mitigation. In addition to ASLR, QuickTime is also getting a feature designed to check the status of the stack buffer. Vista itself has a few extra lines of defense in comparison to its predecessor and in addition to ASLR, including stack buffer overrun detection, SafeSEH exception handling protection, no eXecute (NX) / Data Execution Prevention (DEP) / eXecute Disable (XD), heap randomization, stack randomization and heap corruption detection.