

By [Mariusz 2007a](#), Technology News Editor

## [Symantec Explains the Vista CSRSS Vulnerability](#)

### *Arbitrary code execution is a possibility*

Exploit code for a vulnerability in the Client Server Run-Time Subsystem impacting the Windows 2000 SP4, Windows Server 2003 SP1, Windows XP SP1, Windows XP SP2 and Windows Vista operating systems has been available since December 20, 2006. On the very same day, Microsoft has confirmed the Windows MessageBox Vulnerability and revealed that the Proof-of-Concept allows for local elevation of privilege. According to security vendor McAfee, PoC has been published in the wild on 29 and 31 December 2007. Peter Ferrie, Senior Principal Software Engineer Symantec Security Response, has commented on the double-free bug in a CSRSS message function, confirming the fact that the flaw indeed impacts Windows Vista, but not in a reliable manner. "Of course, that the bug isn't reliable on Vista doesn't mean that everyone can relax. The bug does affect earlier versions of Windows, where arbitrary code execution is far easier to achieve. Is it likely to be exploited? Oh yes," predicted Ferrie. Ferrie explained that although a successful exploit of the Windows MessageBox Vulnerability will most likely produce a denial of service, the execution of arbitrary code cannot be ruled out. "Why the fuss? Simply put, successful exploitation of the bug allows even the most restricted user-mode application to elevate its privileges to the System level. From there, the kernel is accessible even on Vista. Even without entering the kernel, System-level privileges allow almost complete control of the system, so the possibilities are limited only by the imagination," commented Ferrie.