

By: February 2007, Technology News Editor

## The Quasi Immaculate Windows Vista

### *But immaculate nonetheless*

Windows Vista has stepped into this world and on store shelves with a quasi immaculate record. Quasi immaculate due to the fact that two vulnerabilities affect the operating system. One[ADMRK=1] is an issue with the Client Server Run-Time Subsystem and the other affects the Windows vista Speech Recognition feature. And although the problems are real, the severity level that can be attributed to either one does not expose the user or the integrity to its data to critical attacks. Microsoft Windows MessageBox Vulnerability has been around since mid-December 2006. On the background of the limited availability of the operating system, this vulnerability has failed to generate any real issues. McAfee ranked it as a medium threat and Microsoft did not rush to patch it. Even after the commercial availability of Vista, this issue is still valid. Still valid but without real impact on Vista users. In the worst case scenario, the MessageBox vulnerability only allows for DoS or local privilege escalation. And Windows Vista has managed to avoid the VLM vulnerability due to the fact that the operating system is compiled with the C compiler available in Visual Studio 2005 that automatically detects integer overflows at runtime, yet another vulnerability has moved to the center stage of the Speech Recognition features. The Windows Vista Speech Recognition Fatal Vulnerability should receive the "joke" security ranking. Microsoft itself revealed that the possibility of such an exploit is only technical. The reality is quite different. Because for a remote attacker to take control of Vista via speech recognition is an absurd scenario. Users are as exposed to the Vista Speech recognition vulnerability only in theory. The fact that attacker could use the speech recognition capability of Vista to take control over the system is highly unlikely. A potential attacker would be limited to voicing commands such as "copy", "delete" or "shutdown." Windows Vista, in its default configuration does not allow for User Account Control to be managed via voice commands, and therefore the limitations make this vulnerability a non-issue. Not to mention, that you would actually be able to hear the exploit! And as this wasn't enough, the Windows Vista Speech Recognition requires a certain clarity of dictation. Also, the speech profiles entered into the operating system have to match those of the attacker. Furthermore, microphone and speaker placement is another variable that constitutes a barrier to this exploit. So, unless you place your microphone next to the high-definition speakers, and train your speech patterns to the voice of the attacker, also allowing for UAC modifications via voice commands, you should be OK. Quasi immaculate, but immaculate nonetheless.