

24 March 2008

By: Marius Oiaga, Technology News Editor

Windows Vista  
Microsoft

## [Latest Vulnerability Attacks Steer Clear of Vista SP1, but Not XP SP3](#)

### *Exploits target the Microsoft Jet Database Engine*

The latest attacks targeting vulnerabilities in Microsoft's software products have steered clear of Windows Vista Service Pack 1. And despite the fact that the Redmond company touted security advancements when it introduced SP1 for Vista, available as of March 18, the fact of the matter is that neither Windows Vista RTM is impacted by exploits targeting a buffer overrun vulnerability in the Microsoft Jet Database Engine. The security flaw can be exploited through Word, Microsoft informed. [Bill Sisk](#), Microsoft Security Response Center Communications Manager, wanted to clarify the situation and revealed that the company had detected "very limited, targeted attack exploiting a vulnerability in Microsoft Jet Database Engine. Our initial investigation has shown that this vulnerability affects customers using Microsoft Word 2000 Service Pack 3, Microsoft Word 2002 Service Pack 3, Microsoft Word 2003 Service Pack 2, Microsoft Word 2003 Service Pack 3, Microsoft Word 2007 and Microsoft Word 2007 Service Pack 1 on Microsoft Windows 2000, Windows XP, or Windows Server 2003 Service Pack 1." Apparently, in addition to Vista RTM and Vista SP1, Windows Server 2003 SP2 is also not vulnerable. This because all three operating systems feature a Microsoft Jet Database Engine that is not impacted by the buffer overrun vulnerability. However, because of the general Windows XP reference made by Microsoft, it is clear that both SP1, SP2 and even the upcoming Service Pack 3 are vulnerable. Still, the company claims that the risk is limited. "The attacker first created a malicious Access file exploiting the unpatched CVE-2007-6026. Next, to bypass Outlook restrictions mentioned before, the .mdb file was renamed with a different file extension (.asd, a video format). With this trick, as clearly showed in the following picture, Access files are no longer blocked by Outlook because the protection triggers just on the file extension and not on the file format itself. The attacker needs only to find a trick to force the MS Jet library to open the file and trigger the vulnerability that will run the malicious shellcode. Some social engineering and a little help from Office applications will work out well in this specific attack," explained [Elia Florio](#), Symantec Security Response Engineer.