

7 November 2007

By: Marius Oiaga, Technology News Editor

Windows Vista  
Editions  
Microsoft

## [Vista Still Breathing as XP Chokes on Latest Vulnerability](#) *Confirms Symantec*

Windows Vista is still breathing as Windows XP is now choking on the latest vulnerability to hit Microsoft's platform. The Redmond company issued a security advisory detailing a flaw residing in the Macrovision SECDRV.SYS driver that ships by default with both Windows XP and Windows Server 2003. Vista was not nominated along with the two operating systems impacted by the vulnerability and security company Symantec backed Microsoft's position revealing that the Redmond company's latest operating system is indeed immune to exploits targeting the flaw. "The original exploit was found in the wild and actively used against Windows-based computers to gain SYSTEM privileges and install additional malware or bypass other restrictions. It wasn't just proof-of-concept code, but a malicious exploit used in real (but limited) attacks. Vista is not affected. Only SECDRV versions shipped with Windows XP and 2003 are. Instead the version shipped with Vista is a completely different driver, reworked and not vulnerable to this attack. We have tested versions of SECDRV.SYS taken from different systems," revealed [Elia Florio](#), Symantec Security Response Engineer. Florio confirmed that only the versions of the driver that shipped with Windows XP and Windows Server 2003 contain the security hole, for which Macrovision is already offering a remedy. So far, Microsoft has not given any specific indication pointing to a possible inclusion of the patch issued with the next batch of security bulletins scheduled for next week. Symantec warned that - despite the fact that the vulnerability is only locally exploitable - attacks could leverage alternative avenues in order to successfully allow for remote code execution. "The exploit can overwrite memory locations in the kernel, so the attacker can execute code in ring-0. This means that bad guys can bypass security restrictions, gain additional privileges, disable security protections, install a rootkit etc", Florio added. "All users should keep in mind that, in a multi-layered defense perspective, it is possible that malware dropped on the system via some other exploit, could potentially take advantage of the SECDRV bug to take further control of the computer and bypass other layers of protection."