

16 August 2007

By: Marius Oiaga, Technology News Editor

Windows Vista
Microsoft

[x64 Vista Driver Signing Does Not Equal Kernel Patch Protection](#) *Says Microsoft*

Driver signing in 64-bit Windows Vista editions does by no means equal Kernel Patch Protection, explained Russ Humphries, a Microsoft senior program manager with the security team focused on the operating system. Humphries stressed the differences between the two technologies in an effort to underscore the fact that the two security mitigations are complementary but not conjoined. The mandatory driver signing and PatchGuard are features introduced in the 64-bit editions of Vista in order to bulletproof the platform's kernel against the loading of unsigned code and the installation of malware with rootkit behavior in the kernel. "Driver signing provides a method to better identify the author/creator of a piece of software or code so that the author/creator can be approached in the event a reliability issue, vulnerability, or malware is discovered. Signing is not designed to confirm the "intent" of signed code (i.e. good or bad), or whether exploitable bugs or malicious code is present. Malicious or exploitable kernel drivers can lead to system compromise beyond disabling of code signing controls, since kernel driver code has access to hardware as well as all programs running as the user," Humphries stated, adding that "Kernel Patch Protection (KPP) helps protect code and critical structures in the Windows kernel from modification by unknown code or data." The differentiation between driver signing and kernel patch protection comes on the heels of Microsoft updating PatchGuard in conjunction with AMS releasing new ATI drivers to replace vulnerable code. The Redmond company emphasized that the kernel patch protection update was not meant to fix any security flaws. "While this updates adds additional checks to Kernel patch protection system, it does not involve a security vulnerability. Known methods that allow the kernel to be patched on systems where Kernel patch protection is enabled require a system to already be compromised by an attacker," commented Joseph Lumia, Account Technology Specialist, Microsoft Enterprise.