

9 January 2008

By: Marius Oiaga, Technology News Editor

[Microsoft Details Windows XP SP3 Secret Changes](#)

And says it's not about security



Windows XP
Microsoft

If you think that all the changes that Microsoft is introducing with [Windows XP Service Pack 3](#) are included into the official overview of the refresh, then you are sadly mistaking. The fact of the matter is that there is simply more than meets the eye, with the third and final service pack for XP, and changes run deep under the hood of the operating system. And while the Redmond company has illustrated the evolution to SP3 by referencing the addition of such functionality, as the MMC 3.0 framework, MSXML6, Windows Installer 3.1 v2, Background Intelligent Transfer Service 2.5, IPsec Simple Policy Update for Windows Server 2003 and Windows XP, Digital Identity Management Service, Peer Name Resolution Protocol, Wi-Fi Protected Access 2, "Black Hole" Router Detection, Network Access Protection and Kernel Mode Cryptographic Module, it has also managed to leave out additional details concerning other areas of the platform. "Windows XP Service Pack 3 (SP3) includes all previously released Windows XP updates, including security updates and hotfixes. It also includes select out-of-band releases, and a small number of new enhancements, which do not significantly change customers' experience with the operating system.(...) Microsoft is not adding significant functionality from newer versions of Windows, such as Windows Vista, to Windows XP through XP SP3. [However] SP3 does include Network Access Protection (NAP) to help organizations that use Windows XP to take advantage of new features in the Windows Server 2008 operating system", Microsoft revealed in [the service pack's overview](#). But, XP SP3 also brings to the table modifications impacting the DCE/RPC - Distributed Computing Environment/Remote Procedure Call. A detailed comparison of the modifications between DCERPC services on XP SP2 and XP SP3 (release candidate) has been published on [Full Disclosure](#). And while the document is mostly unintelligible outside of professionals, Microsoft managed to detail the XP SP3 range check, denying that it was hiding an overflow condition. "We have received a few inquiries about the full disclosure posting [over [Windows XP SP3 - DCERPC Changes](#)], where a range check was added in Windows XP SP3 for the Terminal Server RPC function RpcWinStationEnumerateProcesses. The speculation stated that this change was to hide an overflow condition, potentially leading to an exploitable vulnerability in previous Windows versions. In reality, this update to the Terminal Service RPC interface definition was made to better adhere to our own RPC best practices", [explained](#) a member of the Security Vulnerability Research & Defense team, subsequently citing the resource for [IDL techniques](#) interface and method design.