

27 November 2007

By: Marius Oiaga, Technology News Editor



[Five-Year-Old Windows Design Flaw Comes Back to Haunt Vista](#)

[Via Windows Proxy Autodiscovery](#)

Windows Vista, Microsoft's latest operating system, has been continually applauded as an apex of security and an epitome of user protection when it comes down to the Windows platforms available on the market. Yet Vista is far from being bulletproof despite the additional security mitigations built into the product from User Account Control to Address Space Layout Randomization. And although Vista is the first product to come out of the Security Development Lifecycle, as a new software building methodology and process designed to tone down the severity and reduce the volume of vulnerabilities, Microsoft still managed to miss some issues. Case in point, a five-year-old design flaw, already discovered and patched by the Redmond company, has come back to haunt Vista, according to New Zealand hacker Beau Butler who presented the vulnerability at the Kiwicon hacker conference in Wellington. Although the security hole has been reported not to affect the U.S. version of Vista, users around the world running the operating system are vulnerable to severe attacks. Butler also revealed that Vista is by no means the sole operating system vulnerable, with the flaw impacting all versions of Windows. The vulnerability is related to the Microsoft WPAD functionality, and involves problems with Windows Proxy Autodiscovery. Butler stated that because of the vulnerability, Windows proxy auto-configuration requests are frequently sent out on the Internet. The flaw essentially allows an attacker to serve false proxy information to vulnerable machines, and in this manner to take over thousands if not million of computers simultaneously. Microsoft confirmed both the vulnerability and its severity, and added that a patch is in the works. However, Microsoft's general manager of product security, George Stathakopoulos, informed that not all Windows machines are vulnerable, and that the configuration of the operating system has a great deal to do with putting its user at risk.