

23 April 2007

By: Marius Oiaga, Technology News Editor

Windows Vista  
Microsoft

## [DNS Vulnerability Not in This Windows Vista](#)

### *Nor in XP*

Microsoft has denied that the critical vulnerability affecting RPC on Windows DNS Server impacts in any way Windows Vista or Windows XP SP2. The Microsoft Security response Center has tested this vulnerability against the complete range of Windows operating systems and has concluded that the issue is limited to Windows 2000 Server Service Pack 4, Windows Server 2003 Service Pack 1, and Windows Server 2003 Service Pack 2. According to Christopher Budd, MSRC Security Program Manager, the Domain Name System (DNS) Server Service vulnerability only impacts the Windows server operating systems. "We know this because as part of our Software Security Incident Response Process (SSIRP) after we identify a vulnerability one of the first things we do is to establish the scope of affected software. We do this looking at the source code for the affected component in all publicly supported versions of the product. We look to see if the code that contains the vulnerability is present in the source code. In the case of this vulnerability, the code with the vulnerability is in the DNS server component. That component isn't present in Windows client operating systems. Because of this, we can say that client systems are not at risk from this vulnerability," Budd stated. Microsoft continued to monitor the evolution of the problem since the initial report on April 12 and confirmed that attacks are still not widespread. Additionally, Budd pointed at May 8, as the official date for a security update to be released. The Redmond Company has also made available a new KB article designed to lend a helping hand to deploy DNS remote RPC block workaround at an enterprise level. "The DNS service listens on RPC over TCP, RPC over named pipes, and LPC. The workaround changes this behavior to listen on LPC only to block any possibility of remote attacks. We know that this has an impact on remote administration requiring a terminal services or console logon to use any admin tools. I assure you that we're working as fast as we can to get a well tested, comprehensive security update out to you all, which addresses the issue. In the meantime, the workaround is good protection against the attacks we've seen so far," stated a member of the SWI team pointing to [KB 936263](#).