

24 October 2008

By: Lucian Constantin, Web News Editor



Windows critical  
vulnerability prompts  
out of cycle patch  
Microsoft Corporation  
(for the original logo)

## [Microsoft Releases Out of Cycle Patch to Fix Critical Remote Code Execution Vulnerability](#)

*The vulnerability affects all supported versions of Windows*

Microsoft usually releases patches once a month, on a day called by the industry the "Patch Tuesday". However, the Redmond company released an unscheduled [advisory](#) along with a patch for a highly critical vulnerability in the Server service, which can be exploited remotely and allow code execution. According to Microsoft's severity rating system, this vulnerability is tagged as Critical for Windows 2000, XP and Server 2003 and Important for Windows Vista and Server 2008.

The vulnerability allows an attacker to completely compromise a system remotely and execute code by sending a maliciously crafted RPC request packet. The vulnerability differs in severity for Windows Vista and Windows Server 2008, because these two platforms require authentication by default in order to execute code. In comparison, on the older platforms, the attacker could achieve this under anonymous credentials.

Windows XP SP2 can be protected if the Windows Firewall is turned on and file/printer sharing is disabled. If any of the two conditions is not met, the operating system is exposed to this attack, because the Server service handles file and printer sharing, which gets added as an firewall exception automatically.

On Windows Vista and Windows Server 2008, the Address Space Layout Randomization ( [ASLR](#) ) plays a very important role in mitigating such attacks by making automatic exploitation nearly impossible. As pointed out on the [Microsoft Security Vulnerability Research & Defense blog](#), "ASLR will randomize the base address of modules, heaps, stacks, PEB, TEBs, etc. making difficult the return into known locations."

[Secunia](#) rates this vulnerability with level 4 (Highly Critical) out of 5 and notes that the vulnerability has been reported as a 0-day (detected in the wild before a patch is released). This is also suggested in the SVRD blog post, which notes that "we have seen targeted attacks using this vulnerability to compromise fully-patched Windows XP and Windows Server 2003 computers." A proof of concept exploit for the vulnerability has already been posted by Stephen Lawler on the exploit tracking website Milw0rm.

All Windows users are advised to deploy the patch immediately, because large-scale computer worms might soon incorporate exploits for this vulnerability and use it to propagate themselves. [Graham Cluley](#), senior technology consultant at Sophos, advises on his blog that "if you're in any doubt about the importance of rolling out the patch - just remember that in the past, hackers have released attacks exploiting security vulnerabilities within hours of Microsoft publishing a fix. Cybercriminals have a window of opportunity to infect computers, and have shown themselves historically not to waste any time."