



[Home](#) | [Forums](#) | [Archives](#) | [Search](#) | [Speedtest](#) | [Advertising](#) | [Contact](#) | [About & Link](#) | [RSS](#)

Links

- [Home](#)
- [Online](#)
- [Discussions](#)
- [Blogs](#)
- [Podcast](#)
- [Downloads](#)

Categories

- [Telecoms](#)
- [Broadband](#)
- [ADSL](#)
- [3G & Cellular](#)
- [MyWireless](#)
- [iBurst](#)
- [Gaming](#)
- [Hardware & Software](#)
- [International](#)
- [Business & General](#)

Sponsor

News Partners

[Home](#) ▸ [Hardware & Software](#)



## 'Dangerous' vulnerability found in Windows

By ICTWorld, 15 August 2006



A 'dangerous' vulnerability has been identified and patched by Microsoft in Windows 2000, Windows XP and Windows 2003 versions.

In the next few days this can lead to attacks on the scale of the 2003 MS Blaster worm, say security analysts at MicroWorld Technologies.

Vulnerability-MS06-040, one among the 23 security holes patched by Microsoft in its latest security bulletin on August 8, is highly critical and poses a direct and dire threat to computers on the Windows platform, the analysts add.

A patch for this vulnerability is available at MS06-040 ( <http://www.microsoft.com/technet/security/bulletin/MS06-040.msp> ) on the Microsoft Web site.

While some of the exploits aimed at the flaw are already available on the Web, and can

### Related Articles

- [Acer takes top spot in SA notebook market](#) 08/15/06
- [Dell recalls 4m laptop batteries](#) 08/15/06
- [Software industry supports AMD's upcoming server chip](#) 08/15/06
- [Apple trading status in jeopardy](#) 08/14/06
- [Dell could face multiple lawsuits](#) 08/11/06
- [IBM's PCs turn 25](#) 08/11/06
- [Microsoft OS dangerously vulnerable](#) 08/11/06
- [BRANDS HOLD ON](#) 08/11/06
- [Creative struggles against iPod](#) 08/11/06
- [Apple unveils Mac Pro](#) 08/10/06

### Sponsor

[Financial Mail](#)

[Business Day](#)

[Business Report](#)

[MoneyWeb](#)

[ICT World](#)

[Finweek/Fin24](#)

[BiA Online](#)

[Mail & Guardian](#)

be used by malware authors, MicroWorld says that a backdoor variant named 'Win32.IRCBot.st' can attack the vulnerability in order to spread through networks.

'Win32.IRCBot.st' is a PE executable that is packed with MEW. It appears as 'wgareg.exe' in the Windows System folder with a description 'Windows Genuine Advantage Registration Service'. The backdoor changes the security settings of the computer, turns off firewall and connects to the remote attacker via IRC channels.

While its first spreading routine is via the AOL Messenger, the second one uses MS06-040 vulnerability to infect remote computers. A hacker can scan for vulnerable IPS as the backdoor sends out the exploit and infect the targeted machine.

“This is just one of the exploits aimed at the vulnerability in question, which can be a curtain-raiser for more attacks in days to come,” says Arti Taru, assistant manager, R&D, MicroWorld Technologies.

“An exploit code pushed through Metasploit Framework can pave way for large scale Denial of Service attacks against unpatched computers. We strongly recommend users to update their Windows versions to prevent any further assaults through this security hole.”

The gravity of the situation can be estimated from the fact that the Department of Homeland Security of the US government has issued an unusual warning on this issue, which says: “Windows users are encouraged to avoid delay in applying this security patch. Attempts to exploit vulnerabilities in operating systems routinely occur within 24 hours of the release of a security patch.”

[Discuss this article](#)

© 2006 MyADSL, All Rights Reserved..



**DataPro**  
INTERNET SOLUTIONS FOR THE REAL WORLD

**Click** and switch to  
**DataPro ADSL for**  
**A faster, more reliable**  
**internet experience**

**News Discussions**

**Advertisement**