

IT BackbonesTM

Security News



**INTERNET CONTENT
RATING ASSOCIATION**

An independent, non-profit organization
whose mission is to protect children
from potentially harmful material

The IT Shield - Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links

- **Home**
- **About**
- **Contact**
- **Submit PR**
- **Search News**
- **What We Can Offer You**
- **IT Events**
- **Time & Money**

Vulnerability In Windows Keeps Computer World On Its Toes

Published 14th August 2006

A dangerous vulnerability is identified and patched by Microsoft in Windows 2000, Windows XP and Windows 2003 versions, which can lead to potential attacks in the scale of the 2003 MS Blaster worm in the next few days, says Security Analysts at MicroWorld Technologies.

Vulnerability-MS06-040, one among the 23 security holes patched by Microsoft in its latest security bulletin on August 08, is highly critical and poses a direct and dire threat to computers on the Windows platform. Patch for this vulnerability is available at MS06-040 (<http://www.microsoft.com/technet/security/bulletin/MS06-040.msp>) on the Microsoft website.

While some of the exploits aimed at the flaw is already available on the web and can be used by malware authors, MicroWorld's Security Analyst informs a new backdoor variant named 'Win32.IRCBot.st' can attack the vulnerability in order to spread in networks.

"Win32.IRCBot.st" is a PE executable that's 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 well 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.”

“Increasing incidents of Zero-Day attacks like these call for a high level of alertness and awareness from all computer users, home segment and Enterprises alike. While we at MicroWorld continue to insulate computers against every new Virus and Worm, it’s extremely important that users too patch their Operating Systems and other software swiftly, to shut the Window of opportunity on the face of the attackers,” affirms Govind Rammurthy, CEO, MicroWorld Technologies.

Company Profiles powered by ITReseller.com

- MicroWorld - [View profile](#)

[Links](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#) | © 2004-2006 IT Backbones Limited

Site developed and hosted by [Design Solution](#) Ltd.