

**SecurityReason**

News from: World

Alert

[News](#)

[Search](#)

[SecurityAlert](#)

[ExploitAlert](#)

[SecurityReason Research](#)

**RSS**

[News](#)

[SecurityAlert](#)

[ExploitAlert](#)

[Apache](#)

[PHP](#)

**Corporate**

[Contact](#)

[About us](#)

**Services**

[SecurePHP](#)

**Note**

» **Topic:** New exploits out for DNS Vulnerability in Windows Server

» **Added by:** Net-Security

» **Date:** 17.4.2007

MicroWorld Technologies urges organizations to be on their guard, as the number of exploits out for the critical DNS vulnerability in Windows Server rose to five. The possibility of "Vanbot" worm exploiting the flaw is also looked into, says the Security firm

The flaw in question was made public by Microsoft last Thursday, as first reports of it came a day after the Redmond firm's Patch Tuesday. The flaw is related to the way DNS (Domain Name System) Server Service uses RPC (Remote Procedure Call) interface.

RPC is a protocol used in requesting a service from a program located in another computer in a network. An attacker can send a malformed RPC packet to create buffer overflow in DNS service, which will allow him to execute arbitrary code on the victim's computer.

The affected versions are Windows 2000 Server Service Pack 4, Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2. Security researchers indicate that the new Windows Server in the making, code named as 'Longhorn', is also not insulated from the danger.

Rohini Sonawane, Chief Operating Officer of MicroWorld, says "If the DNS service is compromised, the intruder can plant Pharming attacks in the computer, where a legitimate web request can be re-directed to a malicious spoof website. It means, when you key in the web address of your bank in a compromised computer, the request will go to the Phishing site, which will capture all your confidential banking information and hand them over to the malware author!"

According to Rohini, a variant of the 'Vanbot' worm known to exploit many earlier Windows vulnerabilities, is reportedly exploiting this new found loophole as well. She said MicroWorld is analyzing these possibilities, even as the firm's products eScan and MailScan safeguard users against all Vanbot varieties.

Vikas Vishwasrao, a Senior Security Analyst at MicroWorld suggests that users of MicroWorld's eConceal firewall can block Port 445 as well as Port 1025 and all Ports above, till Microsoft releases a patch for the flaw, since these Ports are used by the RPC protocol. He said an infection can be sensed using TCP Connection feature of MicroWorld products, as affected computers will show frantic network activity in IRC traffic as well as a huge increase in HTTP traffic on non standard ports.

**Microsoft Windows  
Animated Cursor Buffer  
Overflow Vulnerability**



- 2007-03-30

Vulnerability can be exploited and results in remote code execution with the privileges of the logged-in user.

**Apache**



» [Apache HTTP Server / Tomcat directory traversal](#)

» [Apache mod\\_rewrite Buffer Overflow Vulnerability](#)

**PHP**



» [PHP 5.2.1 with PECL phpDOC local buffer overflow](#)

» [PHP session.save\\_path open\\_basedir Bypass Vulnerability](#)

» [PHP 4 zip\\_entry\\_read\(\) Integer Overflow Vulnerability](#)

If you have found a vulnerability, please send to our SecurityAlert Database : [secalert@securityreason.com](mailto:secalert@securityreason.com)

Also if you have new ( 0-day ) exploit, please send to our ExploitAlert Archive : [exploit@securityreason.com](mailto:exploit@securityreason.com)

---

» [PHP mail\(\) Header Injection Through Subject and To Parameters](#)

---