



GFILANguard
Network Security Scanner

**Download Your
FREE Trial Today!**



- ABOUT US
- CONTACT
- ADVERTISE

[// Learn about the current state of e-mail security in the latest HNS Podcast //](#)

NEWS

- [Off The Wire](#)
- [Security](#)
- [World](#)
- [Virus Center](#)

ARTICLES

- [Latest Articles](#)
- [Reviews](#)
- [Interviews](#)
- [Book Chapters](#)

SOFTWARE

- [Windows Linux](#)
- [Mac OS X](#)
- [Pocket PC](#)

VULNERABILITIES

- [Vendor Advisories](#)
- [Vulnerability Database](#)

EVENTS

- [Webcasts](#)
- [Conferences](#)

NEWSLETTER

- [Subscribe](#)
- [Current Issue](#)
- [Archive](#)

HOME

- [E-MAIL ALERTS](#)
- [SEARCH](#)
- [RSS](#)

OFF THE WIRE **SECURITY WORLD**

- [How security companies sucker us with lemons](#)
- [Hackers invited to break into Philippine Internet voting system](#)
- [Student loan companies illegally use US database](#)
- [How hackers got Washington](#)
- [Single-victim spam attacks skyrocket](#)
- [Top 10 Internet crimes of 2006](#)
- [Microsoft: DNS patch to come by May 8... maybe](#)
- [Q1 Spam trends report: botnets continue sending massive amounts of spam](#)
- [New version of SecureTrack firewall operations management solution](#)
- [TK Maxx highlights database risks, sends warning to UK National Identity Register Project](#)
- [Tips to protect tax filers from online threats](#)
- [Critical vulnerability affecting Akamai Download Manager](#)

LATEST ARTICLES **VIRUS CENTER**

- [Microsoft Information Protection](#)
- [Hacking the Cisco NAC - NACATTACK](#)
- [HNS Podcast: The Present State of E-mail Security](#)
- [The Rise of SSL VPNs](#)
- [JavaScript Malware for a Gray Goo Tomorrow!](#)
- [Instant messaging worm spreads via Skype messages](#)
- [Cimuz.EL, a new and already widespread trojan](#)
- [Worm spreads in the guise of a Security Update](#)
- [Two worm "families" make up most botnets](#)
- [Combined Spamta and Spamtload attack and the look at Grum.A worm](#)

SECURITY SOFTWARE



• [++ GFI LANguard Network Security Scanner 8](#) • [Secrets Protector Pro 2006](#) • [Tracks Eraser Pro 6.1](#) • [Generic Security Service 0.0.19](#) • [Clean Disk Security 7.5.6](#) • [Digital Invisible Ink Toolkit 1.5](#) • [LockNote 1.0.3](#) • [GFI LANguard Network Security Scanner 8](#) • [WinSCP 4.0.0](#) • [ZoneAlarm 7.0.0337](#) • [Outpost Firewall Pro 4.0.1007.7323](#)
• [TrouSerS 0.2.9.1](#) • [FreeRADIUS 1.1.6](#) • [MIMEDefang 2.62](#) • [GnuPG 2.0.3](#) • [strongSwan 4.1.1](#) • [pam_usb 0.4.0](#) • [Wsh 2.2.2](#) • [vthrottle 0.60](#) • [SmokePing 2.0.9](#) • [Nagios 3.0a3](#) • [Tinc 1.0.7](#) • [Keychain 2.6.8](#)
• [Random Password Generator 1.6.1](#) • [Radmin Assistant 1.0.0](#) • [PDFKey Pro 3.4.1](#) • [MultiAlarm 3.4.2](#) • [Mac GPG 1.4.7](#) • [Little Snitch 1.2.4](#) • [iStumbler 98](#)
• [IPSecuritas 3.0rc3](#) • [GlowWorm FW Lite 1.5.3](#) • [FrameSeer 1.7.2](#) • [iProtector 1.3](#) • [Data Guardian 1.1](#)
• [SecuBox for Pocket PC](#) • [Crippin 2.12](#) • [Aircanner Mobile Encrypter 2.9](#) • [Sentry 2020 2.9](#) • [WiFiFoFum 2.1.1](#) • [AirFix 1.0b](#) • [Confidential Notes 1.1](#) • [Aircanner Mobile Firewall 2.4](#) • [WiFi Graph 0.3 RC3](#) • [SignWise Pro 2.52](#) • [eWallet 4.0](#) • [Pocket Warrior 15022003-B](#)

ADVISORIES **VULNERABILITIES**

• [Ubuntu Security Notice - libx11 vulnerability \(USN-453-1\)](#) • [Gentoo Linux Security Advisory - MadWifi: Multiple vulnerabilities \(GLSA 200704-15\)](#) • [Gentoo Linux Security Advisory - File: Denial of Service \(GLSA 200704-13\)](#) • [Turbolinux Security Announcement - Multiple vulnerabilities in xorg-x11, XFree86](#) • [Mandriva Linux Security Update Advisory - cups \(MDKSA-2007:086\)](#) • [Mandriva Linux Security Update Advisory - freeradius \(MDKSA-2007:085\)](#)
• [Pie Cart Pro affiliates.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro orders.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro events.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro index.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro articles.php Inc_Dir Variable Remote File Inclusion](#) • [Pie Cart Pro faqs.php Inc_Dir Variable Remote File Inclusion](#)

GFI: Improved network security & vulnerability scanning with GFI LANguard 8. FREE trial - download today!

New exploits out for DNS Vulnerability in Windows Server Posted on 17 April 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.

[[Security World main page](#)]

↓ **VIDEO: MICROSOFT INFORMATION PROTECTION**

Meeting the Most Urgent Challenges
Facing the Commercial, Government,
Banking, Energy & Telecom Sectors

STRATEGIC INFORMATION SECURITY

23-25 May * Singapore
27-29 May * Dubai

[Home Security](#)

[Security software Australia](#)

[security cameras](#)

[Security Cameras](#)

[Computer Security Audit](#)

[Asset Tracking](#)

Kaspersky **Antivirus** Software

[GFI EndPoint Security](#)

[POS Software & Systems](#)

//COPYRIGHT 1998-2007 BY HNS CONSULTING LTD. // [READ OUR PRIVACY POLICY](#) //