

## Protect, Then Fix, All Internet-Exposed Microsoft Windows Servers

John Pescatore, Richard D. Stiennon

A security flaw threatens nearly all Internet-exposed Windows servers. Enterprises should immediately ensure that all Windows computers are protected or disconnect them until protections are in place.

## NEWS ANALYSIS

---

### Event

On 16 July 2003, Microsoft confirmed the existence of a major security flaw in every version of the Windows operating system based on NT 4.0 code, including Windows XP, Windows 2000 and the recently released Windows Server 2003. The flaw could enable an attacker to take control of a Windows-based computer using an Internet connection. Microsoft is offering a patch at <http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>.

### Analysis

Gartner rates the risk level of this latest Windows vulnerability "Very High" (for further details, see "Internet Vulnerability Risk Rating Methodology"). Nearly every version of Windows used by enterprises is affected by this flaw, which allows simple, unsophisticated scripted attacks on vulnerable servers.

Those enterprises that are following standard "Deny all except that which is explicitly allowed" practices should already be blocking ports 135, 139 and 445 and other affected ports at the enterprise firewall. However, this vulnerability affects desktop operating systems, as well, making it likely that attacks via cable modem, DSL (digital subscriber line) and WLAN (wireless local-area network) "hot spot" Internet connections will impact PCs that are not protected by enterprise firewalls. The vulnerability also lends itself to blended attacks that use malicious software infecting corporate desktops via e-mail to attack Windows servers from inside the firewall. All PCs should have centrally managed personal firewalls installed and configured to shield vulnerable services.

Enterprises should respond to this flaw by:

- Scanning all Internet-exposed servers and disconnecting all exposed servers from the Internet until firewall shielding and vulnerability patching are completed.
- Following Gartner's standard advice to enterprises using Windows 2003 Server not to expose sensitive applications to Internet connections until the first quarter of 2004, because new vulnerabilities unique to Windows Server 2003 will likely be discovered.

**Analytical Sources:** John Pescatore and Richard Stiennon, Gartner Research

### Recommended Reading and Related Research

- "Microsoft's Security Is Improving, but Products Will " — Microsoft has significantly raised the security level of its software, but the effectiveness of its efforts won't be known until new products ship in 2003. **By John Pescatore**
- "Microsoft Security Flaws Highlight Urgent Need for Personal Firewalls" — A stream of new Microsoft security flaws make personal firewalls a critical enterprise requirement. **By John Pescatore**

(You may need to sign in or be a Gartner client to access all of this content.)

## REGIONAL HEADQUARTERS

---

Corporate Headquarters  
56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

European Headquarters  
Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

Asia/Pacific Headquarters  
Level 7, 40 Miller Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

Latin America Headquarters  
Av. das Nações Unidas 12.551  
9 andar—WTC  
04578-903 São Paulo SP  
BRAZIL  
+55 11 3443 1509