

Block and Patch New Microsoft Vulnerabilities Now

Michael A. Silver, Mark Nicolett, John Pescatore, Richard D. Stiennon

Newly discovered flaws in the same area of Windows code exploited by the MSBlast worm show the urgent need for robust firewall blocks and patches.

NEWS ANALYSIS

Event

On 10 September 2003, Microsoft acknowledged the existence of major new flaws in every version of the Windows operating system based on Windows NT 4.0 (NTW4) code, including Windows XP, Windows 2000 and the recently released Windows Server 2003. The company offers a patch and an updated free scanning tool for these flaws (see www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-039.asp).

Analysis

These newly identified vulnerabilities appear in the same RPC (remote procedure call) subsystem exploited by the MSBlast worm, which recently shut down PCs and servers around the world. Microsoft has rated the new vulnerabilities as "critical." Gartner agrees and believes that the new vulnerabilities will be exploited — and that exploits will appear even more rapidly than MSBlast did.

Enterprises must *immediately*:

- Implement firewall policies to block access to these vulnerabilities
- Perform basic quality assurance testing of the patch
- Ensure rapid installation of the patch on servers and PCs

Enterprises 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. But this vulnerability also affects desktop operating systems, thereby opening up PCs unprotected by enterprise firewalls to attacks via cable modem, DSL (digital subscriber line) and wireless LAN "hot spot" Internet connections. The vulnerability also lends itself to blended attacks that use malicious software infecting corporate desktops via e-mail to attack servers from inside the firewall. All PCs should have centrally managed personal firewalls installed and configured to shield vulnerable services.

Despite its considerable experience in documenting Windows vulnerabilities and releasing patches, Microsoft needs to improve in two areas:

- **Communication:** Patches may be incompatible with some configurations or applications, so Microsoft should include a list of affected applications with each fix and update it as newly affected applications are discovered. Having better information on problems that may occur will help enterprises apply patches more quickly.
- **NTW4 support:** Microsoft has released an NT4 server patch for this vulnerability, but Microsoft no longer supports NTW4. Many enterprises still use NTW4, and the many closely related server platforms will require very similar fixes. For this reason, Microsoft should officially commit to supplying critical security fixes for NTW4 through the end of 2004.

This announcement follows a disclosure the previous week of several vulnerabilities affecting every version of Office since Office 97. This stream of recent vulnerabilities — affecting virtually every Windows desktop and server — shows that enterprises urgently need robust blocking capabilities and tools to deploy fixes.

Analytical Sources: Michael Silver, Mark Nicolett, John Pescatore and Richard Stiennon, Gartner Research

Recommended Reading and Related Research

- "MSBlast and a Model for Threat Response" — This widespread worm is a textbook example of the evolution of a threat and the layered strategy needed to respond. **By Mark Nicolett, John Pescatore and Richard Stiennon**
- "Worm Outbreak Shows Need to Keep Paying for Security" — Enterprises must continue to fund basic security measures. **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