

## Prepare for Yet Another Critical Windows Vulnerability

John Pescatore, Martin Reynolds, Richard D. Stiennon

A huge security flaw, which Microsoft has known about since July 2003, means enterprises must once again block and patch all Windows servers and PCs.

## NEWS ANALYSIS

---

### Event

On 10 February 2004, Microsoft acknowledged a critical security flaw in all versions of the Windows operating system. The vulnerability affects a technology called abstract syntax notation (ASN), which enables computers to share data and is used by many Windows security processes. eEye Digital Security reportedly informed Microsoft privately about the ASN flaw in July 2003 to give the company an opportunity to take remedial action. A patch for the flaw is now available at [www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS04-007.asp](http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS04-007.asp).

### Analysis

Gartner believes this latest Windows vulnerability — a "Very High" risk, according to Gartner's Internet Vulnerability Risk Rating Methodology (see below) — presents attackers with the opportunity to unleash another MSBlast-class worm outbreak. Many Microsoft and third-party components use the ASN module. It is remotely accessible through multiple ports and vulnerable to direct execution of attachments. Enterprises must once again undertake the extremely expensive process of patching all Windows-based PCs and servers.

This flaw and the one that made possible the devastating MSBlast attack appear in Windows 2003 Server. Outside security companies — not Microsoft — discovered both flaws; this shows the inadequacy of Microsoft's highly publicized efforts to find vulnerabilities in its software. Gartner has advised enterprises against using Windows Server 2003 in sensitive Internet-exposed applications before 2Q04. We may have to revise even this cautious position if Microsoft fails to commit publicly to extraordinary efforts to eliminate glaring holes in its operating systems. Enterprises should continue to heavily weight the cost of continually patching Microsoft products when deciding which operating system to purchase.

**Recommendations:** To avoid the mass attacks that will almost inevitably attempt to exploit this vulnerability within the next few weeks, enterprises must *immediately*.

- Install the Microsoft patch on *all* PCs and servers
- Block vulnerable ports as they are identified
- Configure enterprise firewalls correctly to limit exposure
- Install personal firewalls on all PCs and intrusion prevention software on all business-critical Windows servers

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

### Recommended Reading and Related Research

- "Internet Vulnerability Risk Rating Methodology" — Gartner offers a simple, actionable method for classifying and prioritizing security vulnerabilities. **By John Pescatore**
- "MSBlast and a Model for Threat Response" — MSBlast offers a textbook example of an emerging threat and an effective enterprise response. **By Mark Nicolett and others**

(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**

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### **Japan Headquarters**

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### **Latin America Headquarters**

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509