

Get Ready for a Sequel to MSBlast

John Pescatore

The continuing stream of Windows vulnerabilities means that enterprises must pay now for strengthened security for their Windows desktops — or pay later for incident cleanup.

NEWS ANALYSIS

Event

On 16 September 2003, two providers of Internet security services, Counterpane Internet Security and iDEFENSE, announced the discovery of malicious code that exploits a recently discovered flaw in most versions of Microsoft's Windows operating system.

Analysis

The huge Windows vulnerability that Microsoft acknowledged on 10 September 2003 provides attackers with all the tools they need to strike enterprises with another worm like MSBlast. The steps many enterprises took for the recent MSBlast attack — and the fact that the newly discovered "exploit" does not specifically target consumer desktops — will limit the impact of the coming attack. However, unprepared enterprises will get hit just as hard as they were by MSBlast.

Enterprises should *immediately*:

- Use Internet firewalls to block the most vulnerable Windows ports: User Datagram Protocol ports 135, 137, 138 and 445 and TCP ports 135, 139, 445 and 593
- Check that Windows services using these ports are not exposed on extranets or DMZs (demilitarized zones)
- Follow Gartner's long-standing advice to install centrally managed personal firewalls on all laptops, and to audit the configurations of these firewalls to ensure that the vulnerable ports are not accepting connections

After taking these protective measures, you should undergo the considerable expense of applying yet another Microsoft security patch (available at www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-039.asp) to every desktop and server running Windows.

Windows has a higher security cost of ownership than other operating systems, and you should budget for the cost of installing personal firewalls, monthly patching and continual vulnerability assessment for all Windows PCs and servers. Include these additional security costs whenever you evaluate the cost of alternative platforms. Also, heavily weight the security track record of software vendors and products when you make procurement decisions.

Analytical Source: John Pescatore, Gartner Research

Written by Terry Allan Hicks, Gartner News

Recommended Reading and Related Research

- "Block and Patch New Microsoft Vulnerabilities Now" — New Windows flaws show the urgent need for firewalls and patches. **By Michael Silver, Mark Nicolett, John Pescatore and Richard Stiennon**
- "Taxonomy of Software Vulnerabilities" — Different types of vulnerabilities require different detection, assessment and mitigation approaches. **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

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