

Rapid Sasser Attack Raises the Cost of Securing Windows

John Pescatore, Mark Nicolett

A fast-moving worm attack exploits the latest vulnerabilities identified in Windows. Enterprises must budget now for intrusion detection for all Windows systems.

NEWS ANALYSIS

Event

On 3 May 2004, media outlets and security firms reported worldwide attacks by a new worm, called Sasser, against Windows-based computers. Sasser exploits a vulnerability in Windows that was acknowledged by Microsoft in an announcement on 13 April 2004. Microsoft is offering a patch for the vulnerability at www.microsoft.com/technet/security/bulletin/ms04-011.msp and a Sasser removal tool at www.microsoft.com/technet/Security/alerts/sasser.msp.

Analysis

The Sasser worm attacks confirm Gartner's prediction that mass worm attacks against the multiple vulnerabilities disclosed by Microsoft on 13 April were likely (see "Latest Microsoft Flaws Stress Need for High-Risk Protection"). In fact, the appearance of this worm makes the shortest time ever — just 18 days — between the appearance of a vulnerability and the beginning of an attack. (Blaster held the previous record, 25 days.)

Many of the vulnerabilities that continue to be identified in Windows 2000, XP and Server 2003 are easily exploitable; attackers will continue to develop worms that will cause damage equal to, or more severe than, the system shutdowns and network congestion caused by the Slammer worm. Enterprises that are dependent on Windows systems must invest both in means to patch faster and in host-based intrusion prevention software for all Windows PCs and servers.

Recommendations:

- **Enterprises that have already invested in configuration management and software distribution systems:** Budget adequate additional funds to expand these efforts to include expedited patching of all Windows PCs and servers.
- **Enterprises that have not yet made investments in configuration management and software distribution:** Allocate funds for patch management systems that can make patching before attacks more feasible, while also ensuring the stability of Windows systems. Simply turning on Windows automatic update feature is not enough.
- **All enterprises:** Recognize that these configuration management and software distribution system or patch management systems must be accompanied by personal firewall, antivirus and behavior-based intrusion prevention software for all Windows PCs and servers. Gartner believes that — even though the market for host-based intrusion prevention software will not be mature until the end of 2005 — enterprises must budget for, and procure, these products now to secure their critical Windows-based systems. The cost and availability of such protection should be included in all total cost of ownership calculations when alternatives to Windows servers and PCs are being evaluated.

Analytical Sources: John Pescatore and Mark Nicolett, Gartner Research

Recommended Reading and Related Research

- "Stay Ahead of Changing Software Vulnerabilities" — Enterprises should adapt their IT security strategies to a changing threat environment. **By John Pescatore**

- "It's Time for Host-Based Security Platforms" — Business-critical platforms require host-based security to protect the expanding enterprise perimeter. **By John Pescatore and Mark Nicolett**

(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