

Patch Security Holes but Demand Better Security From Vendors

John Pescatore

Security holes continue to appear in products from major vendors. Enterprises should apply patches immediately, but vendors will not improve security unless enterprises pressure for them to do so.

NEWS ANALYSIS

Event

On 13 December 2001, Microsoft announced a patch for the most recently discovered security holes in Internet Explorer (IE) v.5.5 and v.6. This vulnerability potentially allows hackers to access user files and to trick users into downloading malicious code. Sun Microsystems and IBM had to issue their own vulnerability alerts and software patches a week earlier when security holes were discovered in their respective Unix server products.

Analysis

The pace of discovery of software vulnerabilities shows no sign of slowing. Microsoft announced what it defines as three critical security flaws in the IE 5.5 and 6 browsers embedded in Windows 2000 and Windows XP. Sun and IBM had to issue patches for Solaris and AIX after a serious buffer overflow vulnerability, which could allow an attacker to log in with "superuser" privileges, was found in those Unix variants. Gartner's Internet Vulnerability Risk Rating method rates both the Windows and the Unix security flaws as "high risk" (see *Research Note* TU-14-9003 "Internet Vulnerability Risk Rating Methodology"). Therefore, enterprises should immediately apply the appropriate vendor patches to all affected servers running AIX or Solaris, and all PCs running IE 5.5 and IE 6.

The odds are high that a worm that uses a Nimda-like approach and that looks to exploit unpatched systems will be launched by the end of 1Q02. To prepare for that threat, enterprises should patch all affected systems as soon as possible and perform backups of server software configurations — that way, the version in backup storage has the patch. They should also update all tools used to monitor configuration compliance to require the latest patched version.

Enterprises should elevate security as an evaluation criterion when deciding about major platform procurements or upgrades. Without market pressure on software vendors to provide more-secure products, enterprises will remain in a vicious cycle of hacks, patches and more hacks. Type B enterprises (adopters of mainstream technology) should not upgrade to new releases of software until at least nine months after general release. Type A enterprises (adopters of leading-edge technology) should require extensive vendor support in security testing before committing to Internet-exposed production use of new releases. Where enterprises hold prototype testing and vendor competitions for new software products, vendors should demonstrate evidence of security testing by outside experts.

Analytical Source: John Pescatore, Information Security Strategies

Written by Dean Lombardo, gartner.com

Need to Know: Reference Material and Recommended Reading

- "Web Server Security Hierarchy" (TG-14-4153). The Code Red worm proved that enterprise attempts to extend old security processes to Web servers have failed miserably. **By John Pescatore**
- "Secure Windows: Oxymoron or on the Horizon?" (SPA-14-7346). Microsoft's Secure Windows Initiative shows promise in reducing vulnerabilities in its server operating systems products. **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