

Microsoft Must Plan -- Not Patch -- for Software Security

John Pescatore

Microsoft released a software patch that fixed security vulnerabilities — but also created new ones. Unless Microsoft changes its basic processes, many of its products will not be secure.

NEWS ANALYSIS

Event

On 7 February 2002, Microsoft announced the release of a major security patch for Internet Explorer that it claimed addressed "all known vulnerabilities" affecting the Web browser. Several hours after making the patch available, Microsoft withdrew it because of an error in the patch itself. On 11 February 2002, Microsoft released a patched version of the patch.

Analysis

The problems with the latest major Internet Explorer patch shows that Microsoft has made security promises it cannot yet keep. In October 2001, Brian Valentine, Microsoft senior vice president for Windows, launched the Strategic Technology Protection Program. Valentine said Microsoft would do "whatever is necessary to ensure the process is complete" and promised a secure Windows 2000 Service Pack by February 2002. The highly publicized "leak" of Bill Gates' memo making security the company's highest priority — and reports that the company's developers have stopped working on new software to test existing code for vulnerabilities — further suggested that Microsoft was finally prepared to take security seriously. However, the news that Microsoft released a major security patch for Internet Explorer without having thoroughly tested it seriously undercuts this impression — and shows that the company has a long way to go in filling the gaps in its approach to software security.

Gartner believes that Microsoft should concentrate its efforts on improving the focus on security in its product management, business, software development and customer support processes. Only then should the company increase the level of security testing of existing code. Security cannot be "tested" into software; it must be a high priority from the start — during requirements analysis and product planning. Microsoft would also do well to order its product management and marketing personnel not to hype the company's newfound "security focus" until they can point to some concrete results. Microsoft needs deployed products that drive the software industry to new security standards, not more failed patches that simply confirm the low security expectations enterprises rightly have had of Microsoft software. Enterprises should make their plans for adoption of new versions of Microsoft software conditional on clear demonstration of more secure products.

Analytical Source: John Pescatore, Information Security Strategies

Written by Terry Allan Hicks, Gartner News

Need to Know: Reference Material and Recommended Reading

- "Secure Windows: Oxymoron or on the Horizon?" (SPA-14-7346). The Secure Windows Initiative shows promise in reducing server vulnerabilities, but questions remain about Microsoft's commitment to security. **By John Pescatore**
- "IIS Web Server Security: Change Products or Processes?" (DF-14-6578). Enterprises using Microsoft's IIS Web server must make serious business decisions to address its known security flaws. **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