

Out-of-Cycle Windows Patch Requires Immediate Action

John Pescatore, Neil MacDonald

Active exploits and a critical Windows vulnerability make a potent mix. Enterprises should expedite patching and shielding to avoid business disruptions.

NEWS ANALYSIS

Event

- On 23 October 2008, Microsoft issued out-of-cycle vulnerability patches for all supported versions of Windows due to the discovery of active exploits against a previously unknown critical Windows vulnerability.
- On 24 October, public exploit code began to become available, increasing the importance of applying the patch. The security bulletin describing the vulnerability is available from Microsoft at <http://www.microsoft.com/technet/security/Bulletin/MS08-067.msp>

Analysis

Microsoft made the right decision to issue an out-of-cycle patch for this vulnerability, given the evidence of active attacks against the Windows Server service and the ease at which exploits can spread across the majority of Windows systems. Although Microsoft reports that these privately reported attacks have been limited and targeted, Microsoft is being very aggressive in pushing these patches out to prevent large-scale downtime for businesses around the world.

This vulnerability is rated "critical" for all Windows XP and older versions of Windows. The security update MS08-67 deals with a vulnerability in the Windows Server service that allows an attacker to remotely execute malicious software on any vulnerable Windows computer. On Microsoft Windows 2000, Windows XP and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code.

The vulnerability is rated only as "important" for Windows Vista and Windows Server 2008. On these newer versions, including Hyper-V on Windows Server 2008 core, authorized access is required. With newer security mechanisms, including processes to address randomization, exploiting vulnerabilities becomes much more difficult.

The vulnerability also increases the risk of attack from malicious worms. Similar vulnerabilities five years ago opened enterprises up to the Slammer and Blaster worms. These worms exploited Windows vulnerabilities and disrupted businesses around the world. Following these incidents, most enterprises implemented vulnerability management processes to rapidly patch Windows PCs and servers. Many more installed network intrusion prevention to block attempts to exploit unpatched Windows systems.

Such protection, combined with Microsoft's investment in a secure software development life cycle process to reduce the number of critical vulnerabilities, has greatly reduced the success rate of attacks trying to exploit these types of vulnerabilities. But these facts have also led to a lessening of the urgency to patch. To ensure business continuity, it is essential to expedite installation of these patches.

RECOMMENDATIONS

All Windows users:

- Patch your systems immediately:
 - Initiate expedited patching processes.

- Prioritize the patching of pre-Vista PCs.
- Run vulnerability scans and network access control health checks with increased frequency this week to ensure patching has occurred.
- If immediate and rapid patching is not possible:
 - Implement monitoring processes to mitigate the risk of a potential attack.
 - Prioritize temporary shielding.
 - Review all personal and network firewall policies to block ports 139 and 445 when not in use.
 - Apply intrusion prevention signatures from IPS vendors for MS08-67 as soon as they are released.
 - Pressure third parties offering hosted and outsourcing services to accelerate patching.

Enterprises on NT4:

- If you don't have Microsoft custom support agreements in place, use firewalls, network or host-based intrusion prevention and hardening techniques to protect vulnerable systems.

Businesses with Windows-based appliances:

- Contact the vendors of any Windows-based appliances, including virtual appliances, such as medical machinery, automated teller machines and process control devices, to determine when the vendor will support the new patches.

RECOMMENDED READING

- "Reducing the Risk of New Threats Requires More Than Fast Patching" — Applying vendor patches is important, but isn't always the highest-priority action in preventing today's attacks. **By Mark Nicolett and John Pescatore**
- "The MarketScope for Vulnerability Assessment" — The vulnerability assessment market is changing as vendors try to evolve to address functional and market challenges. **By Kelly Kavanagh and others**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

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