

More Port 445 Activity Could Mean Security Trouble

John Pescatore

An apparent increase in scanning activity may signal an impending malicious-code attack exploiting a critical Windows vulnerability. Take immediate steps to ensure that the affected Windows port is secure.

NEWS ANALYSIS

Event

On 17 June 2005, media reports indicated that security vulnerability sensors have noted an increase in activity on TCP Port 445, which is associated with Microsoft Windows' Server Message Block (SMB) Protocol. This port could potentially be used to exploit the Microsoft Incoming SMB Packet Validation Remote Buffer Overflow Vulnerability (MS05-27), a critical flaw for which Microsoft released a patch on 14 June.

Analysis

The apparent increase in scanning on Port 445 is a serious concern for enterprise security managers, because it may indicate an impending mass malicious-code attack. Such attacks typically follow a highly predictable timeline:

1. A security vulnerability is identified and a patch is released.
2. Attackers use the patch to reverse-engineer the vulnerability.
3. Exploit code is developed and circulated on the Internet.
4. Attackers scan to find vulnerable systems.
5. A mass attack is launched.

The Port 445 activity may indicate that — in the week since Microsoft released the Windows patch — attackers have reached the fourth state in this process and may be preparing a mass attack employing the widely used SMB protocol.

Recommendations:

- Accelerate your efforts to ensure that all Windows systems are patched.
- Implement shielding or other "workarounds" until patching is complete.
- Immediately review all firewall policies (including those covering personal firewall software) to ensure that Port 445 access is blocked wherever possible.
- Update all intrusion prevention system filters (both network- and host-based) to block attempts to exploit this vulnerability.

Analytical Source: John Pescatore, Gartner Research

Recommended Reading and Related Research

- "Improve IT Security With Vulnerability Management" — Vulnerability management processes can be automated with technology from four main categories of vendors. **By Amrit Williams and Mark Nicolett**
- "Understanding the Nine Protection Styles of Host-Based Intrusion Prevention" — The host-based intrusion prevention systems on the market use markedly different approaches. The best implementations will use multiple techniques. **By Neil MacDonald**

(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
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