

Exploit Code Helps Hackers, Not Enterprises

John Pescatore

The release of exploit code for a major security flaw shows that vendors should release fixes rapidly and that enterprises should not reward irresponsible conduct.

NEWS ANALYSIS

Event

On 24 March 2003, a research scientist in Venezuela released code (apparently created by an unnamed third party) that could be used to exploit a previously identified major security vulnerability in Internet Information Server (IIS). Microsoft acknowledged the existence of the vulnerability and released a patch for it on 17 March 2003. (The patch is available at <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-007.asp>.)

Analysis

The release of exploit code confirms Gartner's Internet Risk Vulnerability Rating of "Very High" for this vulnerability, because it makes unskilled attacks significantly easier. System administrators rarely need exploit code to secure or test their operational systems. Any consultancy or vendor that releases exploit code is attempting either to gain publicity or to increase business by increasing the odds of a successful attack. Enterprises should not do business with consultancies or vendors that conduct business in this manner.

Releasing exploit code is almost never an aid to security, but releasing vulnerability and fix information as early as possible almost always does result in an increase in security. System administrators need the patch and vulnerability information before they can start implementing fixes. Attackers are, however, constantly testing software for new vulnerabilities. If they begin exploiting vulnerabilities before system administrators address them, they have a huge advantage. Vendors should release vulnerability and patch information for critical vulnerabilities as soon as the patch has been developed and tested.

Analytical Source: John Pescatore, Gartner Research

Written by Terry Allan Hicks, Gartner News

Recommended Reading and Related Research

- "Latest IIS Flaw Shows 'Security Through Obscurity' Doesn't Work" — The rapid exploitation of the IIS security vulnerability shows that vendors must release patches as soon as they are available and tested. **By John Pescatore**
- "Internet Vulnerability Risk Rating Methodology" — Enterprises should use the Gartner risk rating method to rapidly rank vulnerabilities. **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