Finally some real coverage of MS

By *CPM*
Created *08/07/2009 - 3:38pm*
Submitted by CPM on Wednesday 8th of July 2009 03:38:05 PM Filed under News [1]

Microsoft warns of serious computer security hole

SAN JOSE, Calif. -

Microsoft Corp. has taken the rare step of warning about a serious computer security vulnerability it hasn't fixed yet.

The vulnerability disclosed Monday affects Internet Explorer users whose computers run the Windows XP or Windows Server 2003 operating software.

It can allow hackers to remotely take control of victims' machines. The victims don't need to do anything to get infected except visit a Web site that's been hacked.

Security experts say criminals have been attacking the vulnerability for nearly a week. Thousands of sites have been hacked to serve up malicious software that exploits the vulnerability. People are drawn to these sites by clicking a link in spam e-mail.

The so-called "zero day" vulnerability disclosed by Microsoft affects a part of its software used to play video. The problem arises from the way the software interacts with Internet Explorer, which opens a hole for hackers to tunnel into.

Microsoft urged vulnerable users to disable the problematic part of its software, which can be done from Microsoft's Web site, while the company works on a "patch" ? or software fix ? for the problem.

Microsoft rarely departs from its practice of issuing security updates the second Tuesday of each month. When the Redmond, Wash.-based company does issue security reminders at other times, it's because the vulnerabilities are very serious.

A recent example was the emergency patch Microsoft issued in October for a vulnerability that criminals exploited to infect millions of PCs with the Conficker worm. While initially feared as an all-powerful doomsday device, that network of infected machines was eventually used for mundane moneymaking schemes like sending spam and pushing fake antivirus software.

http://tech.yahoo.com/news/ap/20090707/ap_on_hi_te/us_tec_microsoft_security

News

Links:

[1] http://www.tuxmachines.org/taxonomy/term/56