



Enter your Zip for a **FREE** home valuation.

Zip Code Submit **HOUSEVALUES**

Dallas, Texas

Welcome, Member! [Visit Member Center](#)

Friday February 13, 2004 6:46 a.m. PST

[Customize](#) | [Make This Your Home Page](#) | [E-mail Newsletters](#) | [MySpecialsDirect](#) | [Subscribe to DMN](#)**News/Home**

- [Local](#)
- [SportsDay](#)
- [Business & Technology](#)
- [Arts & Entertainment](#)
- [GuideLive](#)
- [Texas Living](#)
- [Opinion](#)
- [Weather](#)
- [Classifieds](#)
- [Texas/Southwest](#)
- [Washington](#)
- [Elections 2004](#)
- [Nation](#)
- [World](#)
- [Education](#)
- [Health/Science](#)
- [Obituaries](#)
- [Religion](#)
- [Travel](#)
- [Break Room](#)
- [Pets](#)
- [Photography](#)
- [Special Reports](#)
- [Columnists](#)
- [Automotive](#)
- [Lottery](#)
- [Corrections](#)

STOCKS: **Dow** 10718.14 | **Nasdaq** 2085.71 | **S&P** 1155.11 | Last updated: 08:39 A.M.

+24.07 

+12.10 

+3.00 

If you use Windows, lock out the new flaw

'Race is on' to fix major breach before hackers invade, analysts say

10:32 AM CST on Thursday, February 12, 2004

By DOUG BEDELL / The Dallas Morning News

If Microsoft Corp. customers do not promptly patch the latest security hole, Internet-connected computers could be subject to an unprecedented wave of attacks and disruptions, security experts said Wednesday.

The software giant released a fix Tuesday for a networking vulnerability that is woven deeply into all computers running Windows NT, Windows 2000, Windows XP and Windows Server 2003.

The hole could allow malicious code to spread with lightning quickness, much like the MSBlast worm that exploded onto more than 120,000 computers last summer in its first 24 hours of life.

Advertising

NO ANNUAL FEE
Express Approval / Pay over time
PLATINUM BUSINESS CREDIT CARD

Click here



OPEN
SMALL BUSINESS NETWORK™

ClassifiedCenter

Search local ads and more!

autocenter

- [Find a car](#)
- [Find a dealer](#)

jobcenter

- [Job seekers](#)
- [Employers](#)

homecenter

- [For Sale](#)
- [New Homes](#)
- [Apartments.com](#)
- [For Rent](#)
- [Place an Ad](#)
- [DatingCenter](#)
- [TicketCenter](#)
- [Classified Main Menu](#)

and...

SUBSCRIBE NOW!

The Dallas Morning News
September 2001

Subscriber Services

Newspaper Ads

Submit

Announcements

DMN Front Page
Stories

DMN Story Archive

Obituary Archive

Computer Corner

 [Video: Watch Computer Corner](#)

 [Microsoft Windows Cyber Security Alert](#)

 [Download Windows security update](#)

 [Computer Corner home page](#)

Unpatched computers could be taken over and used to launch Web site attacks, spawn e-mail and delete data.

"There's just a massive amount of potential with this kind of vulnerability," said Ken Dunham, director of malicious code for the iDefense intelligence firm. "It's embedded all over the place."

Added Patrick Hinojosa, chief technical officer of Panda antivirus software: "Now the race is on. The question is whether people will get patched in time before some sociopath puts out the exploit."

It is a question of when – not if – a malicious coder will strike, some experts say. No exploit code has been seen yet. But the vulnerability is so large and tempting, it is doubtful that worm writers will be able to ignore it, they say.

The holes used by most worms are limited to specific programs running on Windows, such as Internet Explorer or the SQL database server.

"But this flaw is an operating system level flaw," Mr. Hinojosa said. "There are many different ways to take advantage of this on most systems. And it would enable administrative-level access, which means you can do anything."

The vulnerability involves a Windows file used by numerous Microsoft programs, including Internet

Explorer, Outlook, Exchange 5, 2000 and 2003, and several versions of the company's line of Internet Information Server software.

Microsoft has been trying to re-emphasize creating secure software with its Trustworthy Computing initiative and has joined with several prominent companies in offering bounties for the capture of those who release exploitative code.

"It could be that the bounties have scared people off and nothing happens with this vulnerability," Mr. Dunham said.

"It might be that the bad guys hold up their hands and say, 'Oh, we don't want to mess with this any more.'

"But I doubt that's going to happen."

Mr. Dunham said iDefense has seen copies of code that successfully crashed an Internet Information Server.

"I'm not saying where we got them, but we tested two different versions," he said. "It would be simple to turn them into a worm."

E-mail dbedell@dallasnews.com