

CLASSIFIED

- Jobs
- Cars
- Homes
- Place a classified ad

LOCAL NEWS
INSIDE NEWS

- Nation/World
- South Florida
- Cuba
- Obituaries
- Traffic
- Lottery results
- Education
- Legislature
- Columnists
- Consumer news
- Condo Law
- News quiz
- News by e-mail

COMMUNITY INFO

- Property Records
- Immigration
- Multicultural Directory
- Next Generation

CHANNELS

SOUTH FLORIDA NEWS

- Broward County
- Palm Beach County
- Miami-Dade County
- Florida
- Nation/World
- Cuba
- Education
- Lotto
- Obituaries

WEATHER

- Hurricane
- Web cam

SPORTS

- Miami Dolphins
- 'Fins Insider Report
- Florida Marlins
- Miami Heat
- Florida Panthers
- High school
- College
- Golf
- Outdoors

BUSINESS

- Local stocks

ENTERTAINMENT

- Movies
- Restaurants
- Festivals
- Music
- TV
- Stage
- Attractions
- Nightlife
- Celebrity news
- Contests

CLASSIFIED

Security flaw discovered in Internet technology

By Ted Bridis
The Associated Press
Posted April 21 2004

WASHINGTON · Researchers uncovered a serious flaw in the underlying technology for nearly all Internet traffic, a discovery that led to an urgent and secretive international effort to prevent global disruptions of Web surfing, e-mails and instant messages.

The British government announced the vulnerability in core Internet technology on Tuesday. Left unaddressed, experts said, it could allow hackers to knock computers offline and broadly disrupt vital traffic-directing devices, called routers, that coordinate the flow of data among distant groups of computers.



The risk was similar to Internet users "running naked through the jungle, which didn't matter until somebody released some tigers," said Paul Vixie of the Internet Systems Consortium Inc.

"It's a significant risk," Vixie said. "The larger Internet providers are jumping on this big time. It's really important this just

gets fixed before the bad guys start exploiting it for fun and recognition."

The flaw affecting the Internet's "transmission control protocol," or TCP, was discovered late last year by a computer researcher in Milwaukee. Paul Watson said he identified a method to reliably trick personal computers and routers into shutting down electronic conversations by resetting the machines remotely.

Experts previously said such attacks could take between four years and 142 years to succeed because they require guessing a rotating number from roughly 4 billion possible combinations. Watson said he can guess the proper number with as few as four attempts, which can be accomplished within seconds.

- Email s
- Print st

[Jobs](#)
[Homes](#)
[Apartments](#)
[Cars](#)
[Personals](#)
[Place a classified ad](#)

SHOPPING

[Advertisers](#)
[Newspaper ads](#)
[Furniture Row](#)

EDITORIALS/LETTERS

[Chan Lowe cartoons](#)

THE EDGE

[Multimedia games and graphics.](#)

HEALTH

TRAVEL

FEATURES/LIFESTYLE

[Food](#)
[Home & Garden](#)
[Books](#)

COMMUNITY

[Calendar](#)

TRAFFIC

[Broward](#)
[Palm Beach](#)
[Miami-Dade](#)
[Maps](#)
[Directions](#)

CORRECTIONS

OTHER SERVICES

[Archives](#)
[Customer service](#)
[News by e-mail](#)

Routers continually exchange important updates about the most efficient traffic routes between large networks. Continued successful attacks against routers can cause them to go into a standby mode, known as "dampening," that can persist for hours.

Cisco Systems Inc., which acknowledged its popular routers were among those vulnerable, distributed software repairs and tips to otherwise protect large corporate customers. There were few steps for home users to take; Microsoft Corp. said it did not believe Windows users were too vulnerable and made no immediate plans to update its software.

Using Watson's technique to attack a computer running Windows "would not be something that would be easy to do," said Steve Lipner, Microsoft's director for security engineering strategy.

Already in recent weeks, some U.S. government agencies and companies operating the most important digital pipelines have fortified their own vulnerable systems because of early warnings communicated by some security organizations. The White House has expressed concerns especially about risks to crucial Internet routers because attacks against them could profoundly disrupt online traffic.

"Any flaw to a fundamental protocol would raise significant concern and require significant attention by the folks who run the major infrastructures of the Internet," said Amit Yoran, the government's cybersecurity chief. The flaw has dominated discussions since last week among experts in security circles.

Copyright © 2004, South Florida Sun-Sentinel

Sun-Sentinel.com

[Questions or comments?](#) | [Paid archives](#) | [Start a newspaper subscription](#) | [How to advertise](#) | [Privac](#)
Copyright 2004, Sun-Sentinel Co. & South Florida Interactive, Inc.