



International Edition |

MEMBER SERVICES

MAKE CNN.com

SEARCH

The Web CNN.com

Search

Enhance

- Home Page
- World
- U.S.
- Weather
- Business
- Sports
- Politics
- Law
- Technology**
- Science & Space
- Health
- Entertainment
- Travel
- Education
- Special Reports

TECHNOLOGY

Report: Flaw could shut down Internet traffic

Researcher exposes router vulnerability

Tuesday, April 20, 2004 Posted: 11:09 PM EDT (0309 GMT)

(CNN) -- Major companies and government agencies are scrambling to ensure they are not vulnerable to an Internet flaw that would allow attacks that could disrupt all communication.

The Department of Homeland Security issued a Technical Cyber Security Alert Tuesday, warning that "sustained attacks" on routers between networks could lead to a "denial-of-service condition that could affect a large segment of the Internet community."

However, the alert also said that normal operations would likely resume shortly after the end of the attack, according to the agency.

The flaw is not new, but it was thought too difficult to exploit until researcher Paul Watson reported finding a way remote attackers could terminate network sessions. He detailed how in his paper "Slipping in the Window: TCP Reset Attacks."

Paul Vixie, president of Internet Systems Consortium Inc., compared the risk to Internet users "running naked through the jungle, which didn't matter until somebody released some tigers," The Associated Press reported.

"It's a significant risk," Vixie told AP. "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."

More typical denial-of-service attacks



Story Tools

- [SAVE THIS](#) [EMAIL THIS](#)
- [PRINT THIS](#) [MOST POPULAR](#)

RELATED

- [Hackers hit supercomputing giants](#)
- [Networking giant's bug could put hackers in the driver's sea](#)
- [National Cyber Alert System](#)
- Britain's [National Infrastructure Security Co-ordination Centre](#)

YOUR E-MAIL ALERTS

- Computer Security
- Computer Networking
- Hackers
- Internet

Search Jobs

Enter Keyword

Enter City

careerbu

Pocket MP3-CD player >

ROCKET EX PANIUM PHILIPS

- SERVICES
- Video
 - E-mail Services
 - CNNtoGO
 - Contact Us

SEARCH

Web CNN.com

ENHANCED BY

PH

We

Audic

Pa

MP3

pock

p

Ultra

Hol

No soft

involved large numbers of computers sending huge amounts of data to routers and overwhelming them.

Activate or [CREATE YOUR OWN](#)

[Manage alerts](#) | [What is this?](#)

Watson's paper showed how an attacker could insert data and trick routers into shutting down network sessions, disrupting a network's communication.

Internet connections between computers are like telephone conversations, explained Jeffrey Guilfoyle, senior security expert at Solutionary Inc. If someone intercepts a call, they could potentially force it to disconnect. A similar situation applies online. In this case, an attacker would need to know specific computer Internet addresses in order to trick the systems into shutting down by resetting them remotely.

It all falls under the realm of "transmission control protocol," or TCP, which works in the background, sort of like traffic laws, to keep Internet data running smoothly.

And while it could be argued there is a flaw in the TCP programming, there is no hole that needs to be patched, such as with a worm or virus, Guilfoyle said.

But security experts believed it would take many years to try the millions of combinations necessary to launch a successful attack. The techniques in Watson's paper suggest it could be accomplished in minutes using only a handful of the combinations.

Guilfoyle said a nefarious hacker would still have to go after a bigger connection that's online for a long period of time, such as a large-scale router.

Routers act like doormen in that they "decide" how Internet traffic gets received and sent by using specific instructions in the TCP.

Many major companies and government agencies should have the necessary protections in place already, said government cybersecurity "czar" Amit Yoran: "The fact of the matter is that ... people who have been concerned about the security of their routers are not susceptible."

"The sky is not falling, and many of the core providers are already on top of this. I don't think ... that we'll see any type of large Internet outage and disruption."

Yoran stressed that home users would not likely encounter any side effects of the flaw. He said this is related mainly to networking, service providers and corporations. Hackers will also need some time to digest this information and plan an effective attack, meaning more problems could arise in the future, he cautioned.

"In my personal opinion, it's highly unlikely that someone surfing the Web tomorrow, who sees a Web site inaccessible ... it's highly unlikely that it's related to today's alert. More likely that time will be required for efficient exploits, for criminals to take advantage of this type of research."

Yoran also said the Department of Homeland Security has been in contact with various international groups and agencies to mitigate the hazard.

Copyright 2004 CNN. All rights reserved. This material may not be published, broadcast, rewritten, or redistributed. [Associated Press](#) contributed to this report.

advertisement

Story Tools

 [SAVE THIS](#)  [EMAIL THIS](#)

[Click Here to try 4 Free](#)

PRINT THIS MOST POPULAR

[Trial Issues of Time!](#)



TECHNOLOGY

TECHNOLOGY NEWS

TOP STORIES

CNN.com HOME PAGE

[Hard disk 'speed limit' found](#)



[NFL player turned soldier killed in combat](#)

- [German pair auction child on Internet](#)
- **CNN/Money:** [Microsoft makes antitrust concession](#)
- [Report: Flaw could affect Web traffic](#)

- [Cleric warns of suicide attacks if U.S. strikes](#)
- [Mortuary photos anger Pentagon](#)
- [100 bodies found in N. Korea train blast](#)

[International Edition](#)

Languages

[CNN TV](#)

[CNN International](#)

[Headline News](#)

[Transcripts](#)

[Preferences](#)

SEARCH

[The Web](#)



[CNN.com](#)



Search

ENHANCED

© 2004 Cable News Network LP, LLLP.
 A Time Warner Company. All Rights Reserved.
[Terms](#) under which this service is provided to you.
 Read our [privacy guidelines](#). [Contact us](#).



All external sites will open in a new window. CNN.com does not endorse external sites.



Denotes premium content.