



[New E-mail alert](#)

- FRONT PAGE
- ENTERPRISE SOFTWARE
- ENTERPRISE HARDWARE
- SECURITY
- NETWORKING
- PERSONAL TECH

SAVED STORIES 0 SEARCH ADVANCED SEARCH

Security

TCP flaw threatens Net data transmissions

Last modified: April 20, 2004, 12:40 PM PDT

By [Robert Lemos](#)
Staff Writer, CNET News.com

- PRINT E-MAIL YOUR TAKE SAVE

A flaw in the most popular communications protocol for sending data on the Net could let attackers shut down connections between servers and routers, according to an advisory released Tuesday by Britain's national emergency response team.

TCP—the Transmission Control Protocol—contains a flaw that "varies by vendor and application, but in some deployment scenarios...is rated critical," said [the advisory](#), published by the United Kingdom's National Infrastructure Security Co-ordination Centre. Networking-hardware maker Juniper Networks has determined that its products are vulnerable. Cisco Systems, Hitachi, NEC, and others are studying the issue, according to the advisory.

Get Up to Speed on...

[Enterprise security](#)

Get the latest headlines and company-specific news in our expanded GUTS section.

The vulnerability allows for what's known as a reset attack. Many network appliances and software programs rely on a continuous stream of data from a single source—called a session—and prematurely ending the session can cause a wide variety of problems for devices. Security researcher Paul

Watson discovered a method that makes disrupting the data flow far easier than previously thought.

The center's advisory is based on security research that Watson plans to present at the [CanSecWest 2004](#) conference this week and apparently had been released a day early by the NISCC, according to the conference organizer. Watson, who runs a prohacking blog at Terrorist.net, could not be reached for comment.

The issue of TCP-related reset attacks has surfaced before—discussions of the flaw on a mailing list for large-network operators dismissed the issue as old news—but they've previously been thought to require the attacker to guess the identifier of the next data packet in a session. The odds on that are about one in 4.3 billion. The NISCC advisory argues that Watson's research shows that any number in a certain window of values will work, making it much more likely that such an attack could succeed.

The effect of resetting a connection varies depending on the application and how resistant the network software is to disruption, the advisory said.

Under certain circumstances, an attack could significantly disrupt the network used by the basic devices of the Internet, known as [routers](#), to map the most

▼ advertisement

Dime

Get Up to Speed

▶ ENTERPRISE SECURITY	▶ VOIP
▶ OPEN SOURCE	▶ WEB SE
▶ UTILITY COMPUTING	▶ WI-FI



Linksys finds its voice
If company founder Vic Gammeter has his way, your next broadband router could resemble a room phone.
▶ [VoIP](#)



Meet the EGA
Donald Deutsch, president of Enterprise Grid Alliance, discusses the new group's focus.
 [PLAY AUDIO](#)
▶ [Utility computing](#)



Minding security
ICSA Labs' Bruce Hugel discusses companies that keep doing the same old thing can't cope about security breaches.
▶ [Enterprise security](#)

efficient data path from one server to another. Known as the **Border Gateway Protocol**, or BGP, the method of passing routing information relies on long-lived sessions, and disturbing those connections could cause "medium-term unavailability," the advisory said.

The flaw could also affect the way special Internet servers, known as name servers, provide the numerical Internet address for a certain domain name, such as cnet.com. Attacks could also be used to disrupt e-commerce, by resetting the secure channels between a browser and a merchant's site.

More on this story's companies and topics

Security

Create alert

Create your own e-mail alert >

Related stories

- ▶ Seeds of destruction
January 15, 2004
- ▶ Mysterious Net traffic spurs code hunt
June 20, 2003
- ▶ Flaws in common software threaten Net
February 12, 2002
- ▶ Flaw found in common Internet standard
May 3, 2001
- ▶ **Get this story's "Big Picture"**

White papers, Webcasts and case studies about security More results

- ▶ Action Steps for Improving Information Security (white paper)
Cisco
- ▶ SAFE: IP Telephony Security in Depth (white paper)
Cisco
- ▶ Managed Security Services Overview (white paper)
Cisco
- ▶ Network Security: Embedded in Network, Integrated in Product (white paper)
Cisco
- ▶ Securing Internal Networks: The Final Frontier (white paper)
Check Point Software

Videos about Security More videos

- ▶ Would you like Wi-Fi with that?
Dave Vucina, CEO, Wayport

Your take

Post a comment

No discussion exists, [click here to start it.](#)

▶ This week's headlines

Latest headlines

- ▶ Monster snaps up German job site
- ▶ Week in review: Net threat—or not
- ▶ HP goes green with handheld discount
- ▶ Scalix raises \$6 million
- ▶ Graphics patent suit targets Dell, others
- ▶ HP remains top chip buyer
- ▶ A patriarch's shadow at troubled CA
- ▶ Earnings alert: AT&T Wireless posts loss
- ▶ AT&T Wireless posts quarterly loss
- ▶ Google's chastity belt too tight
- ▶ IBM expands search push with Masala
- ▶ Ericsson reports strong quarterly profits
- ▶ Software maker plays mobile hand
- ▶ Linux backers foresee desktop gains
- ▶ GPL gains clout in German legal case

Most popular headlines

- ▶ BayStar: SCO needs new management
- ▶ Internet speed record set
- ▶ Shhh! The FBI's listening to your keystrokes
- ▶ Portal envy strikes AOL
- ▶ EU report takes Microsoft to task
- ▶ A year old, Opteron serves notice
- ▶ Apple's Jobs nixes iPod partnerships
- ▶ Microsoft hires key rival from SuSE Linux
- ▶ New tool designed to block song swaps
- ▶ Microsoft to Linux: 'Bring it on'



CNET NEWSLETTERS

CLICK ON A TITLE BELOW TO LEARN

- News.com Morning Dispatch sample
- News.com Afternoon Dispatch sample
- News.com Enterprise Hardware sample

All News.com newsletters

SPECIAL OFFERS FROM OUR PARTNERS

CLICK ON A TITLE BELOW TO LEARN MORE

- Surveys
- IT Professionals
- IT Management
- Small Business Owners

▶ SIGN UP NOW

Manage My Newsletters

Sponsored Links

- ▶ **Secure IP Services**
Secure your Layer 2 Network with SprintLink Solutions. Join Now!
www.sprintbiz.com
- ▶ **VoIP got you down?**
About VoIP standards, measurements, and achieving 99.999% uptime.
www.siemon.com
- ▶ **TCP/IP Hands On Training**
Real World Training in TCP/IP Group Discounts and Onsite Classes
www.trainingcity.com

[How to advertise](#) | [Send us news tips](#) | [Contact us](#) | [Corrections](#) | [XML](#)
[Linking policy](#) | [Content licensing](#) | [News.com mobile](#) | [Newsletters](#) | [E-mail alerts](#)

[FRONT PAGE](#)

[ENTERPRISE SOFTWARE](#)

[ENTERPRISE HARDWARE](#)

[SECURITY](#)

[NETWORKING](#)

[PERSONAL TECH](#)

Featured services: [BNET: Business White Papers](#) | [Find tech jobs](#) | [CNET's Digital Living](#) | [Free magazine trial](#) | [Hot D](#)

[CNET.com](#) | [CNET Download.com](#) | [CNET News.com](#) | [CNET Reviews](#) | [CNET Shopper.com](#)

[GameSpot](#) | [mySimon](#) | [Search.com](#) | [TechRepublic](#) | [ZDNet](#) | [International Sites](#)

Copyright ©2004 CNET Networks, Inc. All Rights Reserved. [Privacy Policy](#) | [Terms of Use](#)

[About CNE](#)