

CNETAsia | [News & Technology](#) | [IT Manager](#) | [Builder](#) | [Product Reviews](#) | [GameSpotAsia](#) | [Downloads](#) ([中文下载](#)) | [Membership](#)



Search

News & Technology



[Systems & Networking](#) | [Applications](#) | [Security](#) | [Communications](#) | [Personal Technology](#) | [Industry](#)

CNETAsia : [News & Technology](#) : [Systems & Networking](#) : TCP flaw threatens Net data transmissions

[Win: Digital Camera](#) • [Sony Micro Vault](#) • [Top news headlines](#) • [IT for small businesses](#) • [SMB IT Forum, 25 May](#) •

TCP flaw threatens Net data transmissions

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

Wednesday, April 21 2004 11:30 AM

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.

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.

▼ advertisement



Latest New

[Linksys founder 'v ambitions](#)

[Asia-Pac PC mark dip in 2004](#)

[Disaster recovery businesses too co](#)

[Intel talks up telec](#)

[Red Hat seeks to case](#)

[TCP flaw threaten transmissions](#)

[For some, new 'gr not compute](#)

[Novell touts Linux innovation](#)

[Microsoft hires ke SuSE Linux](#)

[Software makers i lockdown](#)

[Flat-panel demanc says](#)

[Microsoft sharpen: tool](#)

[Open ICQ interfac target developers](#)

[Sony revises earn](#)

[Former MP3.com online home](#)

[Internet speed rec](#)

[More online servic S'pore NSmen](#)

[S'pore's 'Silicon V power outage](#)

[S'pore IT firms gei China](#)


[Hollywood's new l campus file swapp](#)

[All headlines](#)

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 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.

[Back to News & Technology](#) 

[E-mail story](#)

[Print story](#)

TalkBack: [Post your comment here](#)

Sponsored Links

- HP Promo [Visit our online store for the latest promotions.](#)
- SAMSUNG [Unveil Samsung X600A, the Flash-Light VGA Camera Phone](#)
- Free Event [CNETAsia SMB IT Forum. All SMBs must attend!](#)
- Win prizes [Get a fantastic HP digital camera, PC or printer!](#)
- Canon [Win the sleek and stylish IXUS i now!](#)
- Sony [Win 1 of 5 Sony Micro Vaults every week!](#)
- Win prizes [Enter to win great prizes in our Fujitsu contest!](#)
- eBay [Exclusive Mastercard featuring Zoe Tay!](#)
- CeBIT Asia [The Event where major purchase decisions are made!](#)



[Home](#) | [SiteMap](#) | [Bandwidth Meter](#) | [Send Us Feedback](#) | [Make CNETAsia your homepage](#)

[About](#)

Copyright © 1995-2004 CNET Networks, Inc. All rights reserved. [Privacy Policy](#).