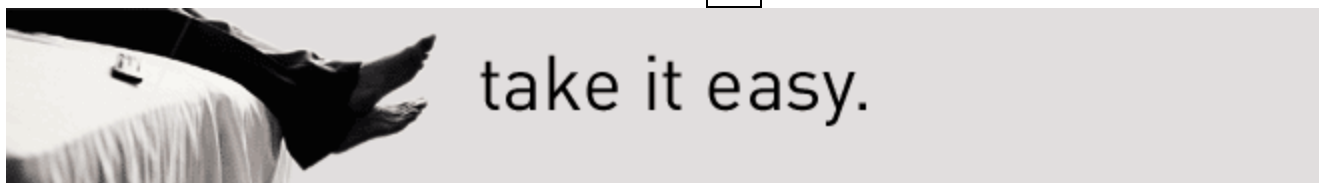


Price Comparison Sho

[+ RP](#)
[NEWS](#)
[INSIGHT](#)
[REVIEWS & PRICES](#)
[DOWNLOADS](#)

[HARDWARE](#)
[SOFTWARE](#)
[INTERNET](#)
[BUSINESS](#)
[COMMENT](#)
[ARCH](#)

[E-COMMERCE](#)
[WEB SERVICES](#)



Search: All of ZDNet

- top search
- newsletters

News > Internet > Security

Wednesday 21st April 2004

TCP hole endangers flow of data

[Robert Lemos](#)
 CNET News.com
 April 21, 2004, 08:45 BST



Tell us your opinion

Britain's national emergency response team has warned that a flaw in the Internet's most popular communications protocol could allow attackers to shut down key connections

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 on 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 centre'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 organiser. 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

Also in News

- Software stops illegal s trading
- Siebel 'meets Google' Cannes
- Microsoft to Linux: 'Bri
- Cisco readies radical c router OS
- Grid grouping draws s
- Job ads suggest Netsc regeneration
- Sex.com's original ovr with VeriSign
- Internet2 sets new spe
- Note-taking tool casts
- Red Hat demands acti case

[More...](#)

Must Read Internet

- Like passwords for ch
- Latest Phatbot angles i server
- Free Google email ser launch 'in weeks'
- Phishing attacks up 1,0 since September

[More...](#)

Internet Features

- Email trails lead to DRI
- Broadband and the city
- Email lists struggle unc avalanche

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 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.

- Cyberwarfare 'a reality in 12 months'
- UK gov't finds security flaws in VoIP and texting technology
- Hi-Tech Crime Unit probes viruses for terrorism links
- Gov't finds open-source flaws

 [Email this](#)  [Print this](#)

TALK BACK

 [Post your message here](#)

[Tell us your opinion](#)

Enjoy this article? Don't miss any of ZDNet's great security content. Security Update gives you comprehensive business intelligence about a variety of security issues delivered straight to your inbox. Subscribe for free weekly updates:

[REGISTER](#)

[Manage my newsletters](#) [More...](#)

■ [Regulators consider th VoIP](#)
[More...](#)

 / [DMM/DDIEDFN](#)

■ "It is good as long as it anonymous and not av any human or ..."
[Read story...](#)

■ "I dont think that the ur have a chance of catch downloading ..."
[Read story...](#)

Internet White Pap

- Close up and personal
 - Microsoft® BizTalk® S Universal Application I
 - XML Backgrounder (U
- [More...](#)

Check Best Prices

- Desktops
 - Notebooks
 - Handhelds
 - Digital Cameras
 - Printers
 - Software
 - Monitors
- [More...](#)