



Part of the **TechWeb** Business Technology Network

**InformationWeek**  
BUSINESS INNOVATION THROUGH TECHNOLOGY

**CMP**  
United Business Media

**Langa Letter: Linux's Achilles' Heel**  
Windows 95 beats Linux

**DaimlerChrysler**  
New add manages p

SEARCH SITE ->

> HARDWARE > SOFTWARE > SECURITY > INDUSTRIES > BUSINESS SERVICES > CAREER DEVELOPMENT

> VIRUSES > ADMINISTRATION > PRIVACY

[SECURITY](#) | [ADMINISTRATION](#)

## Security Vulnerability Threatens Internet April 20, 2004

**A new set of security flaws involving the Transmission Control Protocol could open corporate networks and the Internet to attacks.**

By George V. Hulme

- EMAIL THIS ARTICLE
- PRINT THIS ARTICLE
- DISCUSS THIS ARTICLE
- WRITE TO AN EDITOR

More Stories on:  
[Administration](#)  
[Security](#)

### RELATED STORIES

- [Cisco Reveals Significant Security Flaw](#) 4/21/04
- [Data Lockdown](#) 4/19/04
- [Real-Time Testing Key To Grid Reliability](#) 4/19/04
- [Controversy Over Sloppy Data Sharing](#) 4/19/04

A serious new security vulnerability that could affect large parts of the Internet as well as corporate networks has been identified by the Department of Homeland Security's National Cybersecurity Division and the U.K.-based National Infrastructure Security Coordination Centre.

The flaw involves the ubiquitous Transmission Control Protocol used for Internet traffic, the two groups warned Tuesday.

Hackers could use the "TCP injection vulnerability" in conjunction with a vulnerability in the Border Gateway Protocol, a widely used routing protocol, to launch denial-of-service attacks that would affect "a large segment of the Internet community," according to the Homeland Security advisory.

Also, because of a "TCP/IP Initial Sequence Number vulnerability," Web sites and Internet services that rely on constant TCP sessions could be attacked and suffer from data corruption, session hijacking, or denial-of-service attacks.

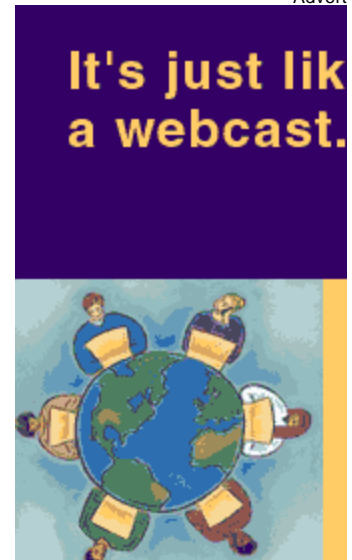
Networking products from Check Point, Cisco Systems, Cray, and Juniper Networks are among those vulnerable because of the flaws, according to the National Infrastructure Security Coordination Centre. More details are available [here](#).

Businesses using equipment from those vendors, some of which have not yet issued patches, should implement IP Security to encrypt network traffic so TCP information won't be available to attackers, reduce the TCP window size, and not publish their source TCP port information, the U.K. security center advises.

To mitigate the BGP flaw, the security center advises companies to filter both incoming and outgoing network traffic to ensure that it has a proper source IP address for the router or firewall receiving the traffic, and to implement the TCP MD5 Signature Option to check the validity of the TCP packet carrying BGP application data. Companies also should limit the amount of information outsiders can gather through domain name system resource records.

Internet Security Systems X-Force, a security resource group, says network infrastructure providers and business networks are the most vulnerable to denial-of-service attacks.

Advert



### CURRENT ISSUE

View all stories from our [current issue](#)



(4/19/2004)

View stories from [past issues](#) sorted by date.

- [EMAIL THIS ARTICLE](#) 
- [PRINT THIS ARTICLE](#) 
- [DISCUSS THIS ARTICLE](#) 
- [LICENSE THIS ARTICLE](#) 

## Mobilize Your Business



[About Us](#) | [Contact Us](#) | [InformationWeek Wireless](#) | [Media Kit](#) | [Shop Our Advertisers](#) | [Editorial Calendar](#) | [Privacy](#)  
[Other CMP Sites](#): | [Optimize Magazine](#) | [Government Enterprise](#) | [Network Computing](#)  
[Healthcare Enterprise](#) | [TechWeb's Technology Pipelines](#) | [InternetWeek](#) | [TechWeb](#)

Copyright