



About Techworld Site Search: News Reviews Features Tech Dictionary You are not currently

Home
 News
 Reviews
 Features
 Storage
 Security
 Mobility & Wireless
 OS and Servers
 Net Management
 Applications
 WANs & Comms
 The BOFH
 Forums
 Network Awards
 Register

Security Knowledge  » [News](#)

21 April 2004

Fundamental Net protocol hole sends vendors diving TCP vulnerability could pose huge problems but it's being worked on

By [Paul Roberts, IDG News Service](#)

A serious [security vulnerability](#) in the fundamental computer protocol TCP has been found by the Infrastructure Security Co-Ordination Centre ([NISCC](#)).

The hole exists in all implementations of TCP that comply with the IETF's spec. By exploiting the hackers could cause TCP sessions to end prematurely, creating a denial of service attack. The also disrupt communications between routers on the Internet by interrupting BGP (Border Gatew that use TCP, NISCC said.

The US-CERT Coordination Center has issued a [warning](#) about the vulnerability. It cites an almc advisory and said that sustained exploitation of the hole could lead to denial of service affecting community."

BGP is the most commonly used routing protocol used by major external routers on the Internet configure redundant high-speed connections and to coordinate with other ISPs and other peers, research director at Internet Security Systems (ISS). "It's the protocol that handles the big pipes

NISCC and US-CERT issued their advisories after a security researcher, Paul Watson, describe called "Slipping in the Window: TCP Reset Attacks." Watson will be presenting the paper at the security conference in Vancouver, Canada, this week.

Watson discovered that the current TCP standard allows a malicious hacker to easily guess a ui needed to reset an established TCP connection because the standard allows sequence number be accepted rather than just exact matches.

By spoofing the source IP address and the TCP port, then randomly guessing the unique seque could cause an active TCP session to terminate.

Networking experts have known about the potential for such attacks for almost 20 years. Howev the use of broadband Internet connections has grown over the years, ISPs and others have gra of the "window", or range of acceptable sequence numbers that they permit to reset a connectio DoS attack more plausible, Ingevaldson said.

BGP sessions are particularly vulnerable to such attacks because they are longer, more predict: often take place between two devices with published IP addresses, he said. "Attackers know wh they're going, they know the ports on either side that are being used and the window," he said.

ISS notified its customers about the hole and said that network infrastructure providers and ente are the most vulnerable to DOS attacks that use the vulnerability.

Leading networking equipment vendors Cisco and Juniper are already on the case, and Cisco h [advisory](#) for its customers that explains the risk in terms of its products.

But despite the dire warnings, the impact of the TCP hole will probably be small, Ingevaldson se

Techworld
 news feeds

Keep up -to-date with
 the latest news and
 features from
 Techworld

Get your Techworld
 headlines here.

TECHWORLD

vendors have probably been in conversation with US-CERT and the NISCC far in advance of their giving those companies time to prepare a patch. Also, the BGP protocol was designed to be resilient to support digital signatures using algorithms such as MD5 that can prevent spoofing, he said.

"This is a serious issue because it's widespread, but there probably won't be a widespread impact

[previous](#)

[Top of Page](#) [Security](#) » [News](#)

Related News »

- » [Vendors must pull up their security socks](#)
[20 April]
- » [Netsky.V climbs through upstairs Windows](#)
[16 April]
- » [Computers infested with spyware and Trojans](#)
[16 April]
- » [Alarm bells ringing as top research centres hacked](#)
[15 April]
- » [Remote access remains top security blackspot](#)
[15 April]
- » [If spam wasn't bad enough, now there's bugged spam](#)
[14 April]
- » [HP servers holed twice](#)
[14 April]
- » [Cisco blunts WLAN hacking tool](#)
[14 April]
- » [Microsoft issues flood of critical patches](#)
[14 April]
- » [Budget cuts mean networks left vulnerable](#)
[13 April]

[More Related News](#)

Related Features »

[Register now](#) for full access to Techworld features!

- » [Adding multicast to IPSec](#)
[20 April]
As multicast applications spread VPNs to work within this environment tunnels are one way.
- » [Safe Bluetoothing](#)
[15 April]
Bluetooth is great, but you still have to be careful when using it.
- » [Fine-tuning Samba for the enterprise](#)
[15 April]
Many tweaks used to fine-tune the fine-tuning of any server. So if your server you can re-use that knowledge.
- » [Defending yourself against port scans](#)
[14 April]
A vital piece of information for administrators on which ports are open on your server.

[More Related Features](#)

TECHWORLD MARKETPLACE

[Precision Internet Filtering Software](#)

Prevent employee Internet abuse automatically with CyBlock software. Web access control plus categorization - one fast, accurate, easy to use solution. Free trial.

[IIS Intrusion Prevention: ThreatSentry ? \\$99.](#)

Neural Intrusion Detection and Prevention Software compares system requests against an evolving baseline of undocumented and other misuse for Microsoft IIS. Small Business Edition, just \$99. Free 30-day trial.

[VeriSign Security Intelligence and Control\(SM\) Services](#)

VeriSign's Security Intelligence and Control(SM) Services let you focus on business initiatives, like record keeping, while VeriSign's experience helps you monitor and manage your security infrastructure.

[Scan All Mail for Viruses and Exploits](#)

Protect your network from e-mail viruses and attacks with GFI MailSecurity - the leading e-mail content checker and exploit detection solution for Exchange and SMTP servers.

[Register for the Free TechNet Flash newsletter.](#)

Get all of the latest Microsoft? IT news and information delivered right to your in-box when you register for this bi-weekly newsletter. This bi-weekly newsletter is designed to help IT professionals stay up-to-date on the latest Microsoft products and events.

[Buy a listing now](#)

Developed, hosted and supported by  BT Limited. Section: security.net