



- Home
- News
- IT Management
- Technology
- MyCW.com
- Career Moves



Logged Out. [Login Here >>](#)

[Advanced Search >>](#)

IT Management

IT Management: Security

by [Bill Goodwin](#)

Tuesday 27 April 2004

Industry races to protect internet from critical flaws

UK government works with telcos in a secret attempt to secure the internet from denial of service attacks

Telecoms companies and internet service providers worked with the UK government in a race to secure the net before news of a serious flaw that could allow hackers to disrupt global internet communications became public last week.

Fourteen communications providers including BT, mobile phone operators and top-tier ISPs worked for six weeks to secure networks in the UK and overseas as part of an international effort to protect the internet.

Business networks remain vulnerable to the problem, which allows hackers to mount denial of service attacks by exploiting weaknesses in the transmission control protocol.

The communications companies, part of a closed group dedicated to sharing information on security problems, accelerated plans to upgrade [network security](#) following confidential warnings from a UK government security agency.

The National Infrastructure Security Co-ordination Centre, which is responsible for co-ordinating the security of the UK's telecoms, transport and communications infrastructure, also tipped off officials in the US, Canada and the Far East.

ISPs and telcos worked with NISCC in a behind-the-scenes operation with a further 150 network and IT equipment suppliers to upgrade the operating systems of thousands of key network routers using the secure MD5 [authentication](#) technology.

Mike Todd, programme director of information assurance at BT, said, "It has enabled us to significantly reduce the risk of the vulnerability before the flaw became public knowledge.

"The worst-case scenario would be widespread disruption of TCP sessions. It had the potential to allow selected or wholesale denial of service attacks."

The industry identified potential problems last year after a group co-ordinated by the NISCC completed a study into vulnerabilities on the internet.

[Print this page >>](#)

[Send to a friend >>](#)

[Subscribe to E-mail >>](#)

N
Sp
Ente
in asso

The de
Project
is here
exclusiv

Gartn
on Co
Be amo
our res
analysis

Sign
to e

Advertis

Microsoft

Roll over to find great IT

10:10 a.m.

1:07 p.m.

Microsoft Office **Get the evaluation**

Advertis

Related Articles

- ▶ [Microsoft holes under further attack](#)
- ▶ [Timms backs online ID scheme](#)
- ▶ [Microsoft patch policy criticised for failure to allow beta testing](#)

Top S
▶ Ger
pus

Major communications firms had already begun a programme to implement MD5 in critical routers, but others had been reluctant because of concerns over cost and the impact on performance, said Roger Cummings, director of the NISCC.

The centre learned in February that security researcher Paul Watson planned to release details of the vulnerability and to distribute code which would allow hackers to exploit the vulnerability.

Officials tried to persuade Watson, who runs a website dedicated to hacking, to postpone publication of a paper to allow telcos and ISPs more time to fix their systems. But he declined, and said that without a deadline, companies would be unlikely to take the problem seriously.

"While I am very strongly in favour of responsible disclosure of vulnerabilities, I also believe that the only way to motivate large businesses is to provide them with the information along with a timescale," he told Computer Weekly.




US accused of ignoring warnings

Security researcher Paul Watson has accused the US of ignoring warnings on the TCP vulnerability.

Watson told Computer Weekly that he reported the problem to UK government security agency NISCC after the US failed to act. He said he originally alerted the US Computer Emergency Response Team in November 2003, but took the matter to NISCC in February after Cert failed to respond.

- [Firms told to patch TCP flaw to protect networks](#)
- [Biometric card scheme will thwart identity theft, says Blunkett](#)
- [International piracy sweep targets 'warez' groups](#)
- [Thought for the day: Stamp out risk](#)
- [UK authorities at centre of crackdown on multimillion-pound software piracy gang](#)
- [ReefEdge fills Cisco's wireless gaps](#)
- [India poised to tighten data protection law](#)
- [Microsoft patch policy criticised for failure to allow beta testing](#)
- [Beware of TCP vulnerability, experts warn](#)
- [Thought for the day: Spam - return to sender](#)
- [Improve default settings, says cybersecurity group](#)
- [Planning priorities](#)
- [In search of cleaner mail](#)
- [Top five threats](#)
- [Opening doors](#)
- [Diary of a penetration tester](#)
- [Move beyond access control](#)

gen
out:
▸ Rea
▸ Tho
Dor
des

-  [Print this page >>](#)
-  [Send to a friend >>](#)
-  [Subscribe to E-mail >>](#)

Our publisher also produces websites covering the following topics:

Banking Information	Travel & Tourism	UK Agricultural Services	Aerospace
Science & Technology	Commercial Property	HR Information	Electronics
Farming & Agriculture	Global B2B Search	Chemical Services & Supplies	B2B Search Engine
Property Information	Hospital & Medical	Catering & Hospitality	Air Transport
Optometry & Optician	Construction Event	Construction & Contractors	Entertainment Search