



Webserver Search

What's that site running?...

Search

Example: [.sco.com](#)
Example: [www.netcraft.com](#)

[RSS feed](#)

Subscribe to Netcraft News

Netcraft Services

Internet Exploration

- [Whats that site running?](#)
- [Search Web by Domain](#)
- [Sites on the Move](#)

Internet Data Mining

- [Hosting Provider Switching Analysis](#)
- [Hosting Provider Server Count](#)
- [Hosting Reseller Survey](#)
- [SSL Survey](#)
- [Web Server Survey Archive](#)

Performance

- [MyDoom Sites](#)
- [Hosting Prospects](#)
- [Performance Alerts](#)
- [Hosting Providers Network Performance](#)
- [Dedicated Server Monitoring](#)

Security

- [Bank Fraud Detection](#)
- [Automated Security Testing](#)
- [Dedicated Server Monitoring](#)
- [Web Application Testing & Site Audits](#)
- [Security Services FAQ](#)

Advertising

[Banner Advertising on Netcraft](#)

About Netcraft

- [About Netcraft](#)
- [Jobs at Netcraft](#)
- [Fair Use, Copyright](#)
- [Site Privacy Statement](#)

« [Previous](#) | [Up](#) | [Next](#) »

Secret Repairs Preceded TCP Flaw Release

Only the math had changed. But the emergence of a workable exploit for an old T hole prompted a secret initiative to fix the Internet, giving network operators a w secure vulnerable routers. The clandestine repair effort livened an already intense security pros already juggling a bevy of Windows security patches.

The [TCP issue](#) publicized yesterday was publicly known as early as 1998. It allows to reset an existing TCP session using specially crafted TCP packets. Most TCP ses short-lived, so the vulnerability has little impact, but certain critical protocols, suc Gateway Protocol (BGP), depend on long-lived sessions. The weakness, which affe used Cisco and Juniper routers, can be addressed by using MD5 authentication to sessions, a step most ISPs had never taken because an exploit seemed mathemat implausible.

[Paul Watson](#) came up with a more efficient way of exploiting the vulnerability, ma attack much faster, particularly for attackers controlling "bot networks" of compro machines. The clock began ticking March 14, when Watson announced plans to pr paper on "specific security problems in the TCP protocol" at the [CanSecWest](#) confe April 21.

Watson shared his plans with government computer security officials in the US an coordinated a response with vendors and major network operators. "We have kno the fixes for about a week and implemented them last weekend," said Bill Hancoc Security Officer for Savvis Communications, which operates the former Cable & W network backbone. Communication was handled through back-channels establishe February 2001 to deploy patches for the SNMP protocol, Hancock said.

The use of MD5 authentication shouldn't affect network performance, Hancock sai an efficient checksum facility and most network operators never operate the core at max capacity, and are intentionally overengineered to deal with situations like 1 as network overloads," he said.

Adding BGP authentication is not a trivial undertaking, however, and network secu were also busy installing critical Microsoft security updates, which took an an urge amid rumors of a Windows "[super exploit](#)". The repair window for the TCP flaw ma shorter than hoped, as [posts to network operator mailing lists](#) suggest the bulletir released a day early due to press attention.

Some network professionals say the TCP issue is overstated. If a hacker with a ne bots desires to take out a router, they argue, it's simpler to overwhelm the device brute force DOS attack than take the time and effort to exploit the TCP weakness. who advocates a [compete overhaul of core Internet protocols](#) to make them more calls it a "medium-level vulnerability." A new [IETF submission](#) proposes small char to address the issue.

Posted by [richm](#) at April 21, 2004 03:00 PM | [Subscribe](#)

« [Previous](#) | [Up](#) | [Next](#) »

[Visiting Netcraft](#)

[Contact Us](#)

[Webmaster](#)

Categories

[About Netcraft](#)

[Around the Net](#)

[Banner Advertising](#)

[Dogfood](#)

[Hosting](#)

[Interviews](#)

[Netcraft Services](#)

[Performance](#)

[Security](#)

[Web Server Survey](#)

[Full Index](#)

Dates

[May 2004](#)

[April 2004](#)

[March 2004](#)

[February 2004](#)

[January 2004](#)

[December 2003](#)

[November 2003](#)

[October 2003](#)

[September 2003](#)

[August 2003](#)

[July 2003](#)

[June 2003](#)

[May 2003](#)

[April 2003](#)

[March 2003](#)

[February 2003](#)

[January 2003](#)

[September 2002](#)

[March 2002](#)

COPYRIGHT © NETCRAFT LTD 2004
