

TECHNOLOGY & SCIENCE

sponsored by



Hacks, Viruses, Scams & Spam

Core Internet technology found vulnerable

Governments scramble to prevent global disruptions

By Ted Bridis

The Associated Press

Updated: 6:54 p.m. ET April 20, 2004

WASHINGTON - Researchers uncovered a serious flaw in the underlying technology for nearly all Internet traffic, a discovery that led to an urgent and secretive international effort to prevent global disruptions of Web surfing, e-mails and instant messages.

The British government announced the vulnerability in core Internet technology on Tuesday. Left unaddressed, experts said, it could allow hackers to knock computers offline and broadly disrupt vital traffic-directing devices, called routers, that coordinate the flow of data among distant groups of computers.

advertisement



"Exploitation of this vulnerability could have affected the glue that holds the Internet together," said Roger Cumming, director for England's [National Infrastructure Security Coordination Centre](#).

The Homeland Security Department issued its own cyberalert hours later that attacks "could affect a large segment of the Internet community." It said normal Internet operations probably would resume after such attacks stopped. Experts said there were no reports of attacks using this technique.

The risk was similar to Internet users "running naked through the jungle, which didn't matter until somebody released some tigers," said Paul Vixie of the Internet Systems Consortium Inc.

"It's a significant risk," Vixie said. "The larger Internet providers are jumping on this big time. It's really important this just gets fixed before the bad guys start exploiting it for fun and recognition."

TCP flaw lets attackers trick routers

The flaw affecting the Internet's "transmission control protocol," or TCP, was discovered late last year by a computer researcher in Milwaukee. Paul Watson said

he identified a method to reliably trick personal computers and routers into shutting down electronic conversations by resetting the machines remotely.

Experts previously said such attacks could take between four years and 142 years to succeed because they require guessing a rotating number from roughly 4 billion possible combinations. Watson said he can guess the proper number with as few as four attempts, which can be accomplished within seconds.

Routers continually exchange important updates about the most efficient traffic routes between large networks. Continued successful attacks against routers can cause them to go into a standby mode, known as "dampening," that can persist for hours.

Cisco Systems Inc., which acknowledged its popular routers were among those vulnerable, distributed software repairs and tips to otherwise protect large corporate customers. There were few steps for home users to take; Microsoft Corp. said it did not believe Windows users were too vulnerable and made no immediate plans to update its software.

Using Watson's technique to attack a computer running Windows "would not be something that would be easy to do," said Steve Lipner, Microsoft's director for security engineering strategy.

Already in recent weeks, some U.S. government agencies and companies operating the most important digital pipelines have fortified their own vulnerable systems because of early warnings communicated by some security organizations. The White House has expressed concerns especially about risks to crucial Internet routers because attacks against them could profoundly disrupt online traffic.

"Any flaw to a fundamental protocol would raise significant concern and require significant attention by the folks who run the major infrastructures of the Internet," said Amit Yoran, the government's cybersecurity chief. The flaw has dominated discussions since last week among experts in security circles.

The public announcement coincides with a presentation Watson expects to make Thursday at an Internet security conference in Vancouver, British Columbia, where Watson said he would disclose full details of his research.

Watson predicted that hackers would understand how to begin launching attacks "within five minutes of walking out of that meeting."

Copyright 2004 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

MORE FROM HACKS, VIRUSES, SCAMS & SPAM

Next →

Hacks, Viruses, Scams & Spam Section Front

- Cisco router flaw could snarl Net
- Core Internet technology found vulnerable
- Con artists target phone system for deaf
- Spyware emerges as new online threat
- Stock-related spam floods e-mail boxes
- Free software sniffs out phishy Web sites
- Hackers target research institutions

- Rush for patches disrupts Microsoft update site
- Microsoft warns of 3 'critical' flaws in Windows
- Junk e-mail has its 10th spamiversary
- Hacks, Viruses, Scams & Spam Section Front

 **TOP MSNBC STORIES**

- Cleric threatens suicide attacks
- N. Korea seeks aid after blast
- Ex-NFL player dies in Afghanistan
- Saddam backers could get rehired
- Battle for Fla. already fierce

 **EDITOR'S CHOICE**

- Traveling with your pet
- MSNBC looks at 'Big Ideas'
- Kwame's Number 2 payoff
- In-flight web links
- Next steps for Mars Rover

advertisement



PENTAX OPTIO 555 \$50 MANUFACTURE REBATE (18273)
-
\$512.99 Sale \$409.95
PENTAX Optio 555 - DIGITAL CAMERAS - 18273
MPsuperstore