

Last Updated on 17:06 AZT- 22 April 2004



National Politics Business World Eurasia Media Tech/Internet Arts & Culture Sp
Opinion

Tech/Internet

Net threat overstated, says security researcher

22/04/2004 16:36

Widespread reports about a flawed communications protocol making the Internet vulnerable to collapse were overblown, according to the researcher credited with uncovering the security problem.

A flaw in the most widely used protocol for sending data over the Net--TCP, or the Transmission Control Protocol--was addressed by most large Internet service providers during the last two weeks and presents little danger to major networks, said Paul Watson, a security specialist for industry automation company Rockwell Automation.

If left unfixed, the weakness could have allowed a knowledgeable attacker to shut down connections between certain hardware devices that route data over the Net.

"The actual threat to the Internet is really small right now," Watson said on Wednesday. "You could have isolated attacks against small networks, but they would most likely be able to recover quickly."

Watson was responding to news reports that ran Tuesday, after Britain's national emergency response team, the National Infrastructure Security Co-ordination Centre, released an advisory about the issue based on his research. Watson, who's scheduled to present that research here at the CanSecWest 2004 conference this week, referred to the media reaction as an "inordinate level of attention in respect to the amount of risk."

At greatest risk, he said, may be e-commerce sites that manage their own routers--those sites may not believe they're vulnerable to attack and may not have implemented a fix. Sites that have routers that share information on the most efficient paths through the Internet--using the Border Gateway Protocol, or BGP--are most vulnerable to the attacks.

Networking-gear maker Cisco Systems said Wednesday that it had released updated software that addresses how the flaw affects its products. Other gear makers, including Juniper Networks, Hitachi and NEC, have been investigating the issue. Information on each company's conclusions can be found in the vendor information section of the NISCC's advisory.

People have known for at least a decade about problems with the way Internet servers and network devices maintain connections with each other. "I am not the first person to notice the issues," Watson said. "I sort of pulled together all the pieces."



- E-Mail this to a friend
- Printable Version
- Add article to Favorites

The problem, said Watson, involves numbers that identify data packets being sent over the Net. Many network appliances and software programs rely on a continuous stream of packets from a single source--called a session. The packets are identified and grouped together using so-called sequence numbers, and, theoretically, if someone could guess the next number in a session and send a packet with that identifier, he or she could substitute illicit commands for authorized ones, Watson said.

The odds against a correct guess were commonly thought to be staggering: about one in 4.3 billion. However--and here's the issue--Watson found that certain applications of TCP sessions, such as routers using the border gateway protocol, relied on long connection times, creating a much larger window of sequence numbers that could be valid. Instead of a one in 4 billion chance to guess the right number, a single-packet attack against a BGP connection might be successful once in 260,000 attempts. An attacker armed with a typical broadband connection could send all 260,000 possible attacks in less than 15 seconds.

It's not simple or elegant, Watson admitted, but it's effective. Rather than unleashing the sort of massive packet flood that normally makes up a denial-of-service attack, an online vandal could send far fewer packets and still bring down a site. "You can take e-commerce sites offline, but instead of billions and billions of packets, you can do it with a whole lot less," he said.

The U.S. Computer Emergency Response Team (US-CERT) has issued an advisory, referencing a similar warning released almost three years ago that mentioned comparable attacks.

Although large Internet service providers are vulnerable "to a very low degree," large and medium-size businesses should make sure they have assessed their vulnerability to the issue, said Sean Hernan, senior member of the technical staff for US-CERT.

"In addition to the core Internet, this TCP vulnerability affects any two endpoints," he said. The vulnerability could affect mail servers, the servers that handle domain names and act as the yellow pages for the Internet, and other major applications. However, in those instances, it is much harder to guess the right sequence numbers, Hernan said.

"This issue turned out to be particularly pernicious against BGP," Hernan said.

Both CERT and Watson recommend that companies add a random 128-bit number to each packet in a session to identify that data as part of the same session--the solution adopted by many major ISPs. Moreover, CERT also recommends that companies encrypt their data to further hide the information in the session from prying eyes.

Source by zdnet.com.com

[15 views]

POST YOUR COMMENT

Name :

E-mail :

Text (Max 1024) :



BakuTODAY.r



Baku Today is a project of **Azer.Net News Ne**
Copyright © 1999-2004 **BAKU TODA**