

The Web: Hackers penetrate network routers

Hackers are now probing a new target -- network routers -- as they seek to wreak havoc on corporate computing networks and evade the extensive security software that has been deployed on PCs and Web servers, experts tell United Press International's The Web.

A router is a device that forwards packets of digital data over networks and is connected to at least two networks, generally local area networks, and wide area networks and the Internet. The routers are located at network gateways, where two networks connect, and have their own operating systems.

The e-mail messages one receives that are sent over the Internet contain "headers" that indicate the path that the data has taken.

"Companies need to work with their vendors and be vigilant in terms of updating their software," Bart Lazar, an intellectual-property attorney based in Chicago with the firm of Seyfarth Shaw, told The Web.

Earlier this month Cisco Systems Inc., the world's largest maker of routers, issued a public advisory about vulnerabilities to its routers a few months after the ability to hack the routers was made public at a conference of hackers, known as the "Black Hat" conference.

"The Cisco Internetwork Operating System (IOS) may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution," said a statement from Cisco.

This router operating system is present in about 80 percent of corporate computing networks.

Attacking routers -- rather than the Internet service provider or a LAN or WAN -- has been, traditionally, difficult, experts said.

"Traditionally, routers have been relatively impenetrable," Ted Demopoulos, IT expert and co-author of the forthcoming book, "Blogging for Business" (Dearborn Trade Publishing, February 2006), told The Web. "They are simpler than operating systems and hence less likely to contain bugs and resulting security flaws. More simple equals more secure."

Another reason that routers have been impervious to attacks in the past is that hackers have known relatively little about them. "The average hacker knows far more about Windows or Unix than routers," said Demopoulos. "It's hard to hack things you don't understand."

That's changing, now, however. Hacking was once a phenomenon powered by pranksters who were looking for some fun at other people's expense.

Now it is a for-profit trade, and the incentives are changing. "Most hacking is for-profit these days," said Demopoulos. "When there is money on the table, anything is open game. Professional hackers concentrate on the bottom line. With Windows and Unix becoming somewhat more difficult to attack, with automated patching and increased security, hackers are considering all options."

Once a security flaw has been discovered in a router, IT departments must be as quick to respond as they are to problems discovered in the other operating systems on their networks, experts said.

Audits of router security are also going to have to be conducted now -- driving up overall IT costs for companies. Response plans for hacker attacks on routers will also have to be developed.

The problem of hacking routers has been developing -- away from the public eye -- for several years now.

According to Andrew A. Vladimirov and Janis Vizulis, co-authors of "Hacking Exposed: Cisco Networks" (McGraw-Hill, December 2005), the presentation this summer by Michael Lynn at the Black Hat confab raised the industry's attention on router hacking.

But the first "public exploit" of routers -- a disclosure of a vulnerability -- is reported to have happened as early as 2001.

Network developers are on the defensive -- claiming that they have the problems under control. But Vladimirov and Vizulis are not so sure. "Router and switch software is still written by humans, and humans do err," the co-authors said in a joint e-mail message to The Web. "Thus, these programs will inevitably have flaws."

There will be more attacks launched and more code that exploits routers written by hackers, Vladimirov and Vizulis predict.

"Some of these attacks will eventually succeed," they told The Web. "Eventually, we foresee that router worms will flourish and join the rest of malware crawling the Internet in search of targets. This will mainly affect the systems that are not looked after properly. This is a situation that is similar to the one in the server world. This does not spell doom for the whole Internet -- it simply means that network administrators will have to stay more vigilant."

Lazar, the intellectual-property attorney, also pointed out that corporate insiders -- not just outside hackers-for-hire -- might also target network routers.

"Therefore, then, another concern is to make sure that your IT staff is not disgruntled," said Lazar, who also recommends that "redundant reporting mechanisms" be put in place on corporate networks "in the event of security breaches, so that more than one person is kept informed."

Copyright 2005 by United Press International

This document is subject to copyright. Apart from any fair dealing for the purpose of private study, research, no part may be reproduced without the written permission. The content is provided for information purposes only.