

The Next Big Target

Cisco routers are everywhere. That makes them your next security concern.

By Larry Greenemeier, [InformationWeek](#)

Nov. 7, 2005

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=173402976>

Which operating system, embedded in more than 80% of enterprise IT environments, represents one of the fastest-growing hacker targets and potentially the most-devastating information-security vulnerability? Hint: It ain't Windows.

Cisco Systems' Internetwork Operating System now sits at the center of the information security vortex. Because IOS controls the routers that underpin most business networks as well as the Internet, anyone exploiting its flaws stands to wreak havoc on those networks and maybe even reach into the computer systems and databases connected to them. IOS is a highly sophisticated piece of software, but--as with Microsoft's Windows--that's a double-edged proposition. Software complexity can be a hacker's best friend.

10

The number of IOS security advisories Cisco has issued in the last two years

Cisco is working hard to better shield its routers and other network equipment from the risks, but there are reasons to believe Cisco security will become a bigger problem before it gets better. The sheer amount of Cisco equipment installed, the many versions of IOS involved, the difficulties of upgrading that software, and the IOS vulnerabilities already out there or yet to be discovered present a major challenge to network administrators and security professionals.

Just last week, Cisco issued a security advisory for a serious IOS "heap-overflow" vulnerability that could let hackers get control of routers and switches running certain versions of the software. Cisco said it's not aware of any "active exploitation" of the vulnerability, which will give customers at least short-term comfort. But Cisco notes that successful exploitations of similar vulnerabilities in the past have resulted in denial of service when the exploit caused a router to crash and reload. "In the event of successful remote code execution," Cisco warns, "device integrity will have been completely compromised."

Proof Positive

This particular problem first came to light in July when information-security researcher Michael Lynn took the podium at the Black Hat conference with a presentation that proved hackers actually could take over IOS, not just shut down Cisco routers. Lynn, who'd been studying IOS code while working for Internet Security Systems Inc., dispelled the widely held notion that it was impossible to exploit IOS buffer overflows to take control of Cisco equipment. He revealed an attack vector in IOS version 12.3(5b) running in IPv6 environments that could be used by hackers to gain control of network traffic; remotely

examine, or "sniff," packet content; modify traffic; and break weak encryption. Lynn went out on a limb to share what he knew, resigning from his job at ISS to make the Black Hat presentation, rather than quiet down. Cisco later obtained a court order to shut him up

Why the fracas? The worry is that cyberpunks could apply what Lynn revealed to gain access to passwords, sneak into networks, or redirect traffic to spoof sites that steal identities. A single point of failure becomes a gateway to all kinds of trouble. "Our networks are becoming very gray with all of the different types of access," says Dan Lukas, lead security architect for Aurora Health Care in Wisconsin, a not-for-profit health-care network with 14 hospitals, 150 clinics, and more than 200 pharmacies. "You don't have any boundary anymore."

On the prospect of future vulnerabilities for router infrastructures, Lukas says, "I see it coming."

Cisco took issue with Lynn's public disclosure, saying it was waiting until it had patches that could be applied to all IOS versions before making an announcement, but it doesn't deny the severity of the vulnerability. "Remote code execution is one of the highest impacts you have, because once you do that, you can do anything on the device," acknowledges Mike Caudill, product security incident manager for Cisco's Product Security Incident Response Team.

Cracking the IOS code to do this kind of harm is harder than hijacking Windows, but Cisco has found it increasingly difficult not only to plug the operating system's security holes but also to get customers to update to the newest versions. The customer heel-dragging is caused by IOS's complexity and by the work involved in upgrading. Over time, Cisco has built many security capabilities into IOS, which is one way to create a secure network, but not the only way. 3Com Corp., for example, lets its Tipping Point intrusion-prevention appliances handle much of the security workload rather than burdening its network operating system. Cisco, meanwhile, keeps layering on more defenses. This month, IOS version 12.4(4)T debuts with deep-packet inspection pattern-matching and filtering capabilities to help companies respond to virus outbreaks.

\$148M

What Cisco spent in the past year to buy three IT-security companies

Complex Upgrades

One consequence of making IOS better is that it also keeps getting bigger. "IOS has become large, monolithic, and bloated with features and functions," says Forrester Research analyst Robert Whiteley. That makes network administrators reluctant to upgrade to the latest version because of the testing and implementation work involved.

Cisco's routers and switches have been built on a variety of processors, including PowerPC and RISC-based chips. As a result, there isn't a single IOS code base that runs on all Cisco products. "That's why Cisco has so many different IOS code trains," says Greg Shipley, chief technology officer of security consulting firm Neohapsis. Juniper Networks Inc., by comparison, has a standardized operating system code base across all of its routers. "It's not that Juniper has never had security problems, but their routers are easier to upgrade than Cisco's," Shipley says.

Here's how it plays out among Cisco's customers. Aurora Health Care uses about 250 Cisco routers, and patching them requires replacing each IOS version with an updated version, then rebooting the system and making sure that the improved IOS doesn't interfere with network

cards or other network devices plugged into the router or switch. "If it's not broken, we don't try to fix it," Lukas says. "We can run the same code on a router for a year."

Lynn's Black Hat presentation showed why such an approach isn't advisable--networks are exposed when router software isn't up-to-date--but there were already warning signs that IOS wasn't bulletproof. Cisco has issued 10 security advisories specific to IOS over the past two years. An April advisory warned that certain configurations might make IOS susceptible to denial-of-service attacks, while another signaled that some versions of IOS could be exploited to permit unauthorized network access. And in May, a Swedish teenager was arrested for using stolen IOS source code to exploit network vulnerabilities and gain access to the National Science Foundation's TeraGrid supercomputing network. The code theft dated back to May 2004, when IOS source code was copied and posted to a Russian Web site.

A Matter Of Time

There hasn't been a successful large-scale attack on Cisco gear. But the exploitation of a major networking vulnerability in an unpatched system will happen, perhaps within a year, now that more people are aware of the type of hack Lynn described, predicts George Roettger, Internet security specialist for regional Internet service provider NetLink Services Inc., which serves Ohio and surrounding areas. "You could now wipe a router clean or reroute traffic through it," he says.

All software makers have bugs in their products that are open to exploitation, Cisco's Caudill notes, and that's true, but beside the point. Caudill says there's a patch for the exploit Lynn demonstrated, and he emphasizes that the exploit applied only to a network specifically running IPv6, which isn't yet widely used in the United States. But with its 128-bit address standard--which supports 340 trillion trillion trillion possible network addresses--IPv6 ultimately will supplant the current Internet address protocol of choice, the 32-bit IPv4, which supports a mere 4.3 billion Internet addresses. Cisco acknowledges there are plenty more potential gotcha's looking for unpatched holes to exploit. "We've seen threats increase 300% over the past few years, from simple viruses to worms that spread at the speed of network connectivity with no human intervention," says Jeff Platon, Cisco's senior director of security product and technology marketing.

1,500

The number of engineers in Cisco's security technology group

Patching IOS is part of the answer, but it's not exactly easy. "To fix it, you have to put a whole new image on a device and restart it," says John Pescatore, VP for Internet security at IT advisory firm Gartner. Cisco generally updates the operating system twice a year, including any new patches, but there's no set schedule for either those releases or individual patches. Competitors 3Com and Juniper Networks tend to issue updates for their less-complex router operating systems as often as four times a year. Still, customers affected by any vulnerability that Cisco discloses are entitled to a free IOS upgrade even if they don't own a maintenance contract, which can run about 20% of the cost of a router.

Easing Complexity

Cisco has taken steps to make patches and upgrades less of a hurdle. Last year, Cisco introduced IOS XR, a modular version of IOS designed specifically for the Cisco CRS-1 Carrier Routing System. IOS XR and CRS-1 took Cisco four years to develop and cost about

\$500 million. IOS XR, created to support the CRS-1's multi-CPU distributed architecture and the requirements of telecom service providers for highly reliable voice and data packet infrastructures, also has been available on the Cisco XR 1200 Series carrier-grade routers since April. This modular design eventually will filter down to other Cisco hardware, including its enterprise-class routers, though the company won't say when.



Complexity in IOS keeps low-level hackers from attacking Cisco's systems, Laidlaw's Turner says.

Photo by Austin Walsh

Not everyone is looking for a stripped-down version of Internetwork Operating System, even if software complexity makes managing it more difficult. "The more complex you make something in the security world, the better it is, so you don't have the script kiddies, or low-level hackers, out there trying to hack Cisco equipment," says Stan Turner, director of infrastructure for Laidlaw Transit Services Inc., an operator of public bus-transportation systems. Building layers of security into networks using firewalls, intrusion-prevention systems, antivirus software, and other components, and rigorous patch management and upgrading, are the price companies have to pay to be secure, Turner says.

Despite the concerns about IOS, or maybe because of them, Cisco's network-security business is booming. The company has expanded its security technology group, which in 2004 reported more than \$1 billion in revenue, to include more than 1,500 engineers. In the past year, Cisco has spent \$148 million to buy network appliance maker FineGround Networks, security and VPN software provider MI Secure, and Protego Networks, a provider of security-monitoring and threat-management appliances. Such moves have broadened Cisco's portfolio of security products and given customers the option of buying layers of security they previously had to get from other vendors.

The rapid growth of Cisco's security business seems to indicate that customers haven't lost faith in Cisco's ability to keep their networks safe. That's even after incidents like the episode in August when Cisco reported that a vulnerability in the search tool on Cisco.com could be exploited to expose passwords for the company's employees, customers, and business partners. The company was forced to reset passwords to remedy the situation.

Even the theft of its operating system code last year didn't shake some customers. "Almost every vendor has an incident with code being stolen if they have enough people working for them," Lukas says.

Cisco's solid reputation overrides any lingering concerns among some customers. The company last year won a contract for the National Law Enforcement Telecommunication System, an interstate law-enforcement network that connects 18,000 local, state, and federal agencies, to replace an aging bisynchronous transmission-based network infrastructure with IP-enabled Cisco routers, switches, and firewalls, as well as an intrusion-prevention system. "I think there's a little bit of concern, but at the same time I believe in Cisco as a company," says Bill Phillips, the network's security specialist.

Cisco's recent bouts with security reinforce the need for constant vigilance--layered security, patch-mindedness, and careful monitoring for unusual patterns that could tip off a security threat. Expect the unexpected, then don't be surprised when it happens.