Cisco Systems

Internet phones sold by Cisco Systems are vulnerable to stealthy hacks that turn them into remote bugging devices that eavesdrop on private calls and nearby conversations.

The networking giant warned of the vulnerability on Wednesday, almost two weeks after a security expert demonstrated how people with physical access to the phones could cause them to execute malicious code. Cisco plans to release a stop-gap software patch later this month for the weakness, which affects several models in the CiscoUnified IP Phone 7900 series. The vulnerability can also be exploited remotely over corporate networks, although Cisco has issued workarounds to make those hacks more difficult.

"Cisco recognizes that while a number of network, device, and configuration based mitigations exist, there is no way to mitigate the physical attack vector on the affected devices," the company's advisory stated. "To this end, Cisco will conduct a phased remediation approach and will be releasing an intermediate Engineering Special software release for affected devices to mitigate known attack vectors for the vulnerability documented in this advisory."

The vulnerability is the latest reminder of privacy threat posed by today's phones, computers, smartphones, and other network-connected devices. Because the devices run on software that is

susceptible to hacking, they can often surreptitiously be turned into listening—and sometimes spying—vehicles that capture our business secrets or most intimate moments.

Hacking Cisco phones.

The vulnerability in Cisco phones was discovered by Ang Cui and Salvatore Solfo, a doctoral candidate and a computer science professor, respectively, in Columbia University's engineering department. In a talk titled "Just because you are paranoid doesn't mean your phone isn't listening to everything you say" and presented at the 29th Chaos Communication Congress, Cui demonstrated a device that connects to the local serial port of a Cisco phone. Once attached, it injects attack code that gives the attacker control over the devices.

Among other things, the hack allows attackers to monitor phone calls and to turn on the phone's microphone in order to eavesdrop on conversations within earshot and stream them over the network.

Cui demonstrated the vulnerability earlier in December. Cisco issued a patch around the same time, but in his later demonstration, Cui said it was ineffective. Cisco responded with Wednesday's advisory, pledging to rewrite the underlying firmware to "fully mitigate the underlying root cause" of the vulnerability. The advisory said that would happen in the next few months but wasn't more specific.

Cui's hack works by overwriting portions of the user or kernel space in the phone's memory. That allows him to gain root access to the phone's Unix-like firmware system and take control of the digital signal processor and other key functions.

While the hack requires physical access to the phone, it would still be possible for janitors, colleagues, or other trusted insiders to carry out the attack. Once done, a phone exhibits few indications that it has been compromised. It's not uncommon for security-conscious people to place masking tape over the video camera of their computers to prevent drive-by attacks that turn them on. Thwarting attacks that turn phones into bugging devices will be harder, since the phones can't be unplugged during calls. Welcome to the world of network-connected devices.