

# The Washington Times

## Insulin pumps, other medical devices vulnerable to computer hackers

[1 Comment and 15 Reactions](#) | | | [Print](#) | [Share](#)[Tweet](#)[Email](#)

By [Shaun Waterman](#)

The Washington Times

Wednesday, October 26, 2011

MIAMI — The special pumps used by hundreds of thousands of diabetes patients are vulnerable to computer hackers, who could make them deliver fatal doses of insulin, security researchers say.

Insulin pumps — like many other medical devices and hundreds of other everyday objects from cars to TVs and refrigerators — are vulnerable because they are controlled by computer chips that can be remotely programmed via a wireless connection.

"I can issue [the insulin pump] any command I like," McAfee security researcher Barnaby Jack told The Washington Times. "I can keep [it] dispensing [insulin] until the pump is empty."

A typical pump reservoir contains about 300 units of insulin. Although exact doses vary among patients depending on body weight and other factors, 10 units would be enough to send someone to the hospital, and 20 units would kill most people.

Mr. Jack demonstrated his ability to take control of an insulin pump from up to 300 feet away at the Hacker Halted conference in Miami, using software he wrote for a normal laptop and an ordinary radio antenna.

He did not make his software available and did not disclose the flaw in the pump he used to take control of it. He said he had shared details of the hack with the maker of the device, but he did not name the company.

A spokeswoman for Medtronic Inc., based in Minneapolis, Minn., confirmed to The Times it was one of the company's pumps that had been hacked.

"We appreciate the security community bringing new information on the possibility of a cyber-attack on our insulin pumps," said Amanda McNulty Sheldon, director of public relations for the firm's diabetes division.

"We have taken a number of steps to address this matter," she added, saying the company is "conducting an in-depth risk/benefit analysis," informing patients and caregivers, and "evaluating the best encryption and security technologies for incorporation into our products."

More than 400,000 of the 25 million diabetics in the U.S. currently use implantable pumps, according to

figures from Research and Markets. Diabetes sufferers cannot produce the hormone insulin, which regulates the level of sugar in the bloodstream.

The pumps, which are about the size of a pager and can be worn on the belt, deliver insulin directly through a tube implanted into the skin.

The wireless remote control feature enables them to link to a glucose monitor that continuously measures the levels of sugar in the blood, so that the pump can deliver insulin as required.

Too much insulin starves the body of glucose, rapidly causing coma and death as the brain shuts down.

Stuart McClure, a senior vice president at McAfee, told The Times there are several ways a hack could be executed.

"This could be used in an [assassination] attempt on a high-profile individual ... or a mass attack by terrorists. We believe those are both credible vectors," he said.

Ms. Seldon said that Medtronic does not believe there is a serious risk of anyone actually using the hack.

"At this time, we believe that the risk is low and the benefits of the therapy outweigh the risk of an individual criminal attack," she said.

Insulin pumps are not the only medical devices that are vulnerable, according to Majid Sarrafzadeh, director of the Wireless Health Institute at the University of California in Los Angeles.

"Many other devices have these kinds of vulnerabilities," he said, including blood pressure monitoring cuffs and pacemakers.

The use of wireless technology in medical devices is increasing, he said, noting that it is an important way to contain rising health care costs because it makes devices more responsive and efficient.

"Unfortunately, because these systems were never the target of hackers before, they were never designed with security in mind," he said. "The danger is immediate."

Ms. Seldon said Medtronic is working to set up an industry working group with representatives from "the diabetes, health care and security community" to help develop better security for medical devices.