By Jim Finkle

Johnson & Johnson is telling patients that it has learned of a security vulnerability in one of its insulin pumps that a hacker could exploit to overdose diabetic patients with insulin, though it describes the risk as low.

Medical device experts said they believe it was the first time a manufacturer had issued such a warning to patients about a cyber vulnerability, a hot topic in the industry following revelations last month about possible bugs in pacemakers and defibrillators.

J&J executives told Reuters they knew of no examples of attempted hacking attacks on the device, the J&J Animas OneTouch Ping insulin pump. The company is nonetheless warning customers and providing advice on how to fix the problem.
“The probability of unauthorized access to the OneTouch Ping system is extremely low,” the company said in letters sent on Monday to doctors and about 114,000 patients who use the device in the United States and Canada.

“It would require technical expertise, sophisticated equipment and proximity to the pump, as the OneTouch Ping system is not connected to the internet or to any external network.”

A copy of the text of the letter was made available to Reuters.

Insulin pumps are medical devices that patients attach to their bodies that inject insulin through catheters.

The Animas OneTouch Ping, which was launched in 2008, is sold with a wireless remote control that patients can use to order the pump to dose insulin so that they do not need access to the device itself, which is typically worn under clothing and can be awkward to reach.

Jay Radcliffe, a diabetic and researcher with cyber security firm Rapid7 Inc, said he had identified ways for a hacker to spoof communications between the remote control and the OneTouch Ping insulin pump, potentially forcing it to deliver unauthorized insulin injections.

The system is vulnerable because those communications are not encrypted, or scrambled, to prevent hackers from gaining access to the device, said Radcliffe, who reported vulnerabilities in the pump to J&J in April and published them on the Rapid7 blog on Tuesday. [bit.ly/2dOUm0e](http://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L)

J&J executives said they worked on the security issues with Radcliffe.

Dosing a patient with too much insulin could cause hypoglycemia, or low blood sugar, which in extreme cases can be life threatening, said Brian Levy, chief medical officer with J&J’s diabetes unit.

Company technicians were able to replicate Radcliffe’s findings, confirming that a hacker could order the pump to dose insulin from a distance of up to 25 feet, Levy said. He said such attacks are difficult to pull off because they require specialized technical expertise and sophisticated equipment.

"We believe the OneTouch Ping system is safe and reliable. We urge patients to stay on
the product," Levy said.

J&J’s letter said that if patients were concerned, they could take several steps to thwart potential attacks. They include discontinuing use of a wireless remote control and programming the pump to limit the maximum insulin dose.

Radcliffe said he believed that OneTouch Ping users would be safe if they followed the steps outlined in the letters from J&J.

"They can give peace of mind to the patient or parent of a child using the device," he said.

FDA GUIDANCE ON MEDICAL DEVICES

In August, a prominent short seller and a cyber security research firm went public with allegations of potentially life-threatening cyber vulnerabilities in heart devices from St. Jude Medical Inc.

As its shares tumbled St Jude said the allegations were false and the U S Food and Drug Administration began an investigation.

RELATED COVERAGE

Johnson & Johnson letter on cyber bug in insulin pump

J&J said before it sent out the letters, it reviewed the matter with the FDA, which is preparing to issue formal guidance on how medical device makers should handle reports about cyber vulnerabilities.

An early draft of that guidance, which was released in January for public comments, called for device makers to work with security researchers, identify steps to mitigate risks, and provide patients with information about bugs so they can "make informed decisions" about device use.

The FDA on Tuesday praised J&J and Rapid7 for their work in discovering, finding ways to mitigate and disclosing the vulnerability.

"This is the proactive behavior the FDA has been looking to see from the medical device manufacturer and research community and demonstrates the collaborative manner in which vulnerabilities can be addressed in a way that best protects patients," the agency said in a statement.

J&J Chief Information Security Officer Marene Allison said her team would make sure other J&J products do not have similar bugs.

Radcliffe said he found vulnerabilities in the Animas OneTouch Ping, but not the Animas Vibe line of insulin pumps.

The FDA has said it knows of no cases where hackers have exploited cyber vulnerabilities to harm a patient.

The agency last year issued multiple warnings about cyber bugs in infusion pumps from Hospira, which has since been acquired by Pfizer Inc. (reut.rs/2duNuZK)

(Reporting by Jim Finkle; Editing by Jonathan Weber and Grant McCool)