Medtronic probes insulin pump risks

Medtronic Inc has asked software security experts to investigate the safety of its insulin pumps, as a new claim surfaced that at least one of its devices could be hacked to dose diabetes patients with potentially lethal amounts of insulin.
While there are no known examples of such a cyber attack on a medical device, Medtronic told Reuters that it was doing "everything it can" to address the security flaws.

Security software maker McAfee, which has a health industry business, exposed the new vulnerability in one model of the Medtronic Paradigm insulin pump on Friday and believes there could be similar risks in others.

Medtronic and McAfee declined to say which model is involved or how many such pumps are currently used by patients. It has two models of insulin pumps on the market and supports six older versions, with about 200,000 currently in use by patients.

The finding points to a broader issue -- the potential for cyber attacks on medical devices ranging from diagnostic equipment to pumps and heart defibrillators, which rely on software and wireless technology to work.

"This is an evolution from having to think about security and safety as a healthcare company, and really about keeping people safe on our therapy, to this different question about keeping people safe around criminal or malicious intent," Catherine Szyman, president of Medtronic's diabetes division, said in an interview.

Szyman, whose nephew uses a wearable Medtronic insulin pump, said the company turned to McAfee rival Symantec Corp and other security firms after an independent researcher exposed less serious vulnerabilities in the pumps in August.

Since then, a research team at Intel Corp's McAfee said it has developed code that allows it to gain complete control of the functions of one Medtronic insulin pump model from as far away as 300 feet.

"We found a way around all the restrictions and all the limitations," said Stuart McClure, a senior vice president with McAfee who heads up the research team.

McClure, formerly a security expert at healthcare giant Kaiser Permanente, says he is exposing such problems to draw them to the attention of manufacturers and regulators.

McClure's team used a Windows PC and an antennae that communicates with the medical device over the same radio spectrum used for some cordless phones.

The type of vulnerability discovered by McAfee could theoretically be used as a new

cyber weapon. A hacker could launch a "drive-by" attack aimed at a high-profile target, such as a politician or corporate executive, who uses this type of insulin pump, McAfee researchers said.

In August, Medtronic acknowledged that security flaws in its implanted insulin pumps could allow hackers to remotely take control of the devices.

The U.S. Food and Drug Administration noted that there is no evidence of widespread problems from medical device security breaches. It says that device manufacturers are responsible for the safety of their software.

"Any system with wireless communication can be subject to interception of data and compromised privacy as well as interference with performance that can compromise the safety and effectiveness of the device," FDA spokeswoman Erica Jefferson said. "We continue to closely monitor for safety or security problems."

HOSTILE ACTORS
Medtronic is a leading makers of insulin pumps along with Johnson & Johnson's Animas Corp and Insulet Corp. McAfee did not report vulnerabilities in models from other manufacturers.

The fresh concerns over the pumps made by Medtronic, the world's largest medical device maker, follow a high-profile recall of heart defibrillator leads in 2007 and a more recent Senate probe into whether doctors it had paid failed to report problems from a spinal surgery product.

The company said it is also consulting with McAfee and has informed patients, through its website, to check their insulin pumps if they have a suspicious encounter with another person.

Medtronic officials have said it would be difficult to make changes to pumps already in use because of FDA regulations that require device makers to get agency approval before altering their products, including issuing software patches.

The company would likely have to first get FDA approval and then recall each pump, which uses wireless communications technology dating back 12 to 15 years, so that technicians could install the new software and check the equipment to make sure that it still accurately delivers doses of insulin.

Szyman said she could not say how long it would take Medtronic to come up with a fix for the vulnerabilities because its investigation is still ongoing. It is also unclear how long it might take the FDA to approve changes to the pumps.

"There's different pathways to approval," she told Reuters, noting that the agency typically takes six to 12 months to approve a new medical device.

Medtronic's diabetes products, which includes its insulin pumps, accounted for more than $1.3 billion in revenue in its last fiscal year, out of a total of nearly $16 billion.

The Medtronic pump vulnerability was discovered by Barnaby Jack, a well-known security expert who joined McAfee last year after gaining notoriety by finding ways to hack into ATMs used at convenience stores, then force them to literally spit out cash. The manufacturers have since fixed the flaw by updating the software that runs those machines.

The nightmare scenario, according to McAfee, involves a hostile actor launching a potentially fatal attack by taking control of an insulin pump, then ordering it to dump all the insulin in its canister.

That is something that was hard to imagine when the product was first designed - long before the recent rash of hacking attacks: "We are talking about code that was written over ten years ago," said Jack. "They never expected anybody to pop these devices open and look under the hood. We are trying to spark some change and get a secure initiative under way and get these devices fixed."

Insulin is a hormone secreted by the pancreas that converts glucose into energy. In patients with diabetes, the body makes no insulin, or insulin levels are too low. This can cause the amount of glucose in the bloodstream to rise, a condition known as hyperglycemia.

When too much insulin is released into the blood stream, a person's blood sugar can become too low, a condition known as hypoglycemia. Symptoms of hypoglycemia range from nausea and confusion to, in severe cases, seizures, coma and death.

McClure declined to say how many models in Medtronic's line of insulin pumps were vulnerable. He said there is no evidence anybody else has identified the flaw or tried to exploit it.

"We just tested one model number," McClure said. "But we believe that more than that are vulnerable." His team demonstrated the vulnerability at a McAfee users conference in Las Vegas on Friday.

McAfee has consulted with experts at the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team, or ICS-CERT. That agency works with private companies in industries including healthcare to help investigate potential cyber vulnerabilities in their products.

Officials with ICS-CERT and Symantec could not be reached for comment.

(Reporting by Jim Finkle in Boston. Additional reporting by Toni Clarke [1] in Boston, Anna Yukhananov in Washington and Susan Kelly in Chicago; Editing by Michele Gershberg [2], Edward Tobin and Martin Howell [3])

Links:
[1] http://blogs.reuters.com/search/journalist.php?edition=us&n=toni.clarke&
[2] http://blogs.reuters.com/search/journalist.php?edition=us&n=michele.gershberg&
[3] http://blogs.reuters.com/search/journalist.php?edition=us&n=martin.howell&