US warns of unusual cybersecurity flaw in heart devices

January 11 2017, by Tami Abdollah And Matthew Perrone

The Homeland Security Department warned Tuesday about an unusual cybersecurity flaw for one manufacturer's implantable heart devices that it said could allow hackers to remotely take control of a person's defibrillator or pacemaker.

Information on the security flaw, identified by researchers at MedSec Holdings in reports months ago, was only formally made public after the manufacturer, St. Jude Medical, made a software repair available Monday. MedSec is a cybersecurity research company that focuses on the health-care industry.

The government advisory said security patches will be rolled out automatically over months to patients with a device transmitter at home, as long as it is plugged in and connected to the company's network. The transmitters send heart device data back to medical professionals.

Abbott Laboratories' St. Jude said in a statement it was not aware of deaths or injuries caused by the problem. The Food and Drug Administration also said there was no evidence patients were harmed.

The federal investigation into the problem started in August.

MedSec CEO Justine Bone said on Twitter that St. Jude's software fix did not address all problems in the devices.

St. Jude's devices treat dangerous irregular heart rhythms that can cause

cardiac failure or arrest. Implanted under the skin of the chest, the devices electronically pace heartbeats and shock the heart back to its normal rhythm when dangerous pumping patterns are detected.

The company's Merlin@home Transmitter electronically sends details on the device's performance to a website where the patient's physician can review the information. But that device can also be hacked.

The FDA's review is ongoing, agency spokeswoman Angela Stark said. Its investigation confirmed the vulnerabilities of the home transmitter, which could potentially be hacked and used to rapidly deplete an implanted device battery, alter pacing and potentially administer inappropriate and dangerous shocks to a person's heart.

The software patch issued by St. Jude "addresses vulnerabilities that present the greatest risk to patients," Stark said.

Stark said the company is working to address remaining vulnerabilities quickly. She said any new cardiac devices submitted to the FDA for review that use the affected transmitter will not be cleared or approved without the software update.

St. Jude disclosed details about the problem after it merged with Abbott. The company has previously denied findings that their devices could be hacked and filed a lawsuit against Muddy Waters LLC and MedSec, alleging that they tried to manipulate the markets to profit from the vulnerability research disclosures.

The revelations about a hacker's ability to potentially gain remote access and affect even the workings of a human heart shed light on the pressing problems of cybersecurity in an increasingly networked world. The advisory also highlights the dilemma for security researchers who may feel an obligation to inform the public of possible dangers but don't want

to cause unnecessary panic.

"Your average patient isn't going to be targeted by assassins," said Matthew Green, an assistant professor for computer science at Johns Hopkins University. He was hired by Muddy Waters to help validate the MedSec findings after St. Jude filed its lawsuit. "An attack on this level is low-probability but very high-impact." He called it "probably the most impactful vulnerability I've ever seen."

Green said many of the more severe vulnerabilities identified by MedSec for the devices themselves have not been fixed, but the new software would make the home system a little more secure.

The FDA has been urging manufacturers to update their products, software and security measures since at least 2013. However, agency guidelines issued last year are not binding. The FDA does not review the vast majority of cyber security updates made to devices, under its own rules intended to streamline medical device upgrades.

In 2015 the FDA issued two separate safety alerts to hospitals over drug pumps made by Hospira, now owned by Pfizer.

In the second notice, regulators told hospitals to stop using the company's Symbiq Infusion System after the company confirmed the system could be remotely hacked, allowing an outside party to potentially reprogram the drug pumps. The devices are used to slowly dose intravenous drugs for pain, infection, nutrition and other uses and are usually programmed through a wireless hospital network.

No patient injuries were reported in connection with the issue, but the agency urged users "to begin transitioning to alternative infusion systems as soon as possible."

Hospira discontinued the pumps for unrelated reasons prior to the FDA announcement, according to the agency.