FDA says pacemakers, glucose monitors and other devices could be vulnerable to hackers

March 5 2020, by Joe Carlson

Credit: CC0 Public Domain

Federal agencies warned patients and manufacturers Tuesday that a recently discovered problem with Bluetooth Low Energy communications may allow computer hackers to remotely disable or

access pacemakers, glucose monitors, ultrasound devices and other medical systems.

The FDA and Homeland Security Department said that while there have been no reports of patients harmed by the problem, the software needed to run such an attack is available online.

Medtronic confirmed Tuesday that some of its products are affected, but said the impact is limited to "temporary disruption of communication function" and would not impact therapy.

The FDA's alert described the potential for much worse problems in other devices. "These cybersecurity vulnerabilities may allow an unauthorized user to wirelessly crash the device, stop it from working, or access device functions normally only available to the authorized user," the FDA's alert said.

Tuesday's alert was triggered by the publication of an academic paper, "Unleashing Mayhem over Bluetooth Low Energy," that outlined at least 12 different security vulnerabilities in devices that use a low-energy version of Bluetooth communication systems. Most of the vulnerabilities would simply crash the systems, but a few would allow a malicious hacker within radio-communication range to insert commands that change how devices function.

Collectively known as "SweynTooth," the flaws affect computer chips from seven different manufacturers that are used in devices, including medical products. Also affected are certain athletic wearable devices, "smart" home-security systems and locks, wireless computer mouses, and others.

"The most critical devices that could be severely impacted by SweynTooth are the medical products," the paper from three authors at

Singapore University of Technology and Design said. "While our team did not verify the extent to which SweynTooth affects such devices ... it is highly recommended that such companies update their firmware. This is to avoid any situation that could pose life-threatening risks to the patients using the respective medical products."

The SweynTooth vulnerabilities allow an unauthorized party to remotely access wireless communications between medical devices that are "paired" over a Bluetooth Low Energy (BLE) connection.

Bluetooth is a common communication system used by wireless devices that talk to each other. Bluetooth Low Energy is a version of that system that requires less energy, which makes it attractive to devices that operate on limited battery power, like medical devices.

Daniel Beard, managing director of the California-based med-tech cybersecurity research firm MedISAO, said each manufacturer of affected devices will have to run its own security assessment because the extent of the impact depends on how the device is assembled.

If the same computer chip inside a device is running both communications and medical-therapy functions, then a SweynTooth hack could affect its medical functionality, Beard said. If communications and therapy are on separate chips, the effect would be limited to disrupting how the device communicates wirelessly with other devices.

Pacemakers, diabetes monitors and ultrasound machines—categories that are specifically called out in the FDA alert—are widely used in health care. Several device companies said Tuesday that they were working to find out more information.

"The FDA recommends that medical device manufacturers stay alert for

cybersecurity vulnerabilities and proactively address them by participating in coordinated disclosure of vulnerabilities as well as providing mitigation strategies," Dr. Suzanne Schwartz, a deputy director in the FDA's Center for Devices and Radiological Health, said in the announcement.

A spokeswoman for Medtronic confirmed Tuesday that several families of products are affected.

"To date, our analysis has confirmed these (vulnerable) hardware components are present in some Medtronic products in both our Cardiac & Vascular and Diabetes product lines. However, our assessment indicates the impact is limited to temporary disruption of communication function and does not impact therapy," spokeswoman Erika Winkels said via e-mail.

Medtronic heart devices affected by the vulnerability are: the Azure portfolio of pacemakers; the Percepta, Serena, and Solera family of cardiac resynchronization therapy pacemakers (CRT-Ps); and the Cobalt and Crome cardiac resynchronization therapy defibrillators (CRT-Ds).

The diabetes products affected by the vulnerability are: the Guardian Connect glucose sensor transmitter, which is part of the Guardian Connect stand-alone glucose monitoring system; the Envision Pro glucose recorder, which is part of the Envision Pro professional glucose monitoring system; and the MiniMed Connect "uploader," which is a secondary display accessory for the MiniMed 530G and MiniMed Paradigm sensor-augmented insulin pumps.

Neither insulin pumps nor its continuous glucose monitoring (CGM) transmitters that communicate to pumps made by Medtronic contain the affected hardware components, the company said.