Two gov notices point to vulnerabilities in devices for heart problems

23 March 2019, by Nancy Cohen

Credit: CC0 Public Domain

The U.S. Department of Homeland Security (DHS) and the U.S. Food and Drug Administration (FDA) issued communications that cybersecurity vulnerabilities were found in some Medtronic devices. Hundreds of Medtronic heart devices are vulnerable to cybersecurity incidents, according to two US federal government notices.

The vulnerability also affected patients' home bedside monitors that read data from the devices and in-office programming computers used by doctors, said *Star Tribune*.

Ana Mulero, *Regulatory Focus*: The FDA issued an FDA safety communication; DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory to flag cybersecurity vulnerabilities. These were detected in Medtronic's Conexus telemetry protocol. "The wireless technology is used to enable communication between the medical device manufacturer's implantable cardiac devices, clinic programmers and home monitors."

Implanted defibrillators are for treating heart problems. They are placed beneath the skin. They deliver electric shocks if an irregular heartbeat is detected, noted *TechSpot.*

Two vulnerability types were mentioned regarding (1) formal authentication or authorization protections, and (2) data encryption. Mulero said, "Improper access was assigned a critical (9.3) score and data transmission has a medium (6.5) vulnerability score."

According to Mulero, "Both FDA and ICS-CERT reported that an attacker or unauthorized individual could exploit the detected cybersecurity vulnerabilities to access one of the affected products in proximity, impact device functionality and/or intercept sensitive patient data within the telemetry communication."

The official website of the Department of Homeland Security posted on Thursday Medical Advisory (ICSMA-19-080-01), Medtronic Conexus Radio Frequency Telemetry Protocol. "The result of successful exploitation of these vulnerabilities may include the ability to read and write any valid memory location on the affected implanted device and therefore impact the intended function of the device."

A list of specific products and versions of Medtronic devices that use the Conexus telemetry protocol that are affected can be found in the medical advisory posting of Thursday, March 21. (A protocol is used to connect monitors wirelessly to an implanted device, said *TechSpot*.)

Homeland described vulnerabilities in different models of Medtronic implantable defibrillators, said *Star Tribune*.

TechCrunch and *TechSpot* discussed some technical details of what sparked the warning. Those devices having wireless or radio-based technology pose the benefit of allowing patients to monitor their conditions and their doctors to adjust

settings without having to carry out an invasive surgery. Medtronic's proprietary radio communications protocol, known as Conexus was not encrypted and there was no authentication process.

Attackers, with radio-intercepting hardware, and within a certain range, could modify data on an affected defibrillator, changing the implant settings.

Hackers would need to be close to users—around 20 feet, noted Rob Thubron in *TechSpot*.

Medtronic in its security bulletin on Thursday informed that "Fully exploiting these vulnerabilities requires comprehensive and specialized knowledge of medical devices, wireless telemetry and electrophysiology."

The *Star Tribune* article carried quotes from Dr. Robert Kowal, chief medical officer for Medtronic's cardiac rhythm and heart failure products. He said that "a hacker would have to be within 20 feet or so of the patient, would need detailed knowledge of the device's inner workings, and have possession of specialized technology to pull off the hack."

What should patients do, then? Medtronic recommended that patients and physicians continue to use these devices as prescribed and intended. "The benefits of remote monitoring outweigh the practical risk that these vulnerabilities could be exploited."

Discussing mitigation, Medtronic said in its bulletin that it was "developing updates to mitigate these vulnerabilities" and will be informing patients and physicians when available subject to regulatory approvals. The medical advisory appearing on the Department of Homeland Security website said that "Medtronic has applied additional controls for monitoring and responding to improper use of the Conexus telemetry protocol by the affected implanted cardiac devices. Additional mitigations are being developed and will be deployed through future updates, assuming regulatory approval."

Thubron in *TechSpot* added that the company was monitoring its network "for anyone trying to exploit the flaws." He said that "the defibs will shut down wireless transmission upon receiving any unusual requests. The company is working on a fix for the vulnerabilities, which should arrive later this year."

Medtronic, meanwhile , stated that "To date, neither a cyberattack nor patient harm has been observed or associated with these vulnerabilities."

In the bigger picture, "Medical device makers have bolstered efforts to mitigate product security vulnerabilities in recent years following a flurry of warnings from security researchers who have identified bugs in devices like the Medtronic implant programmers," said Reuters.

More information:
www.fda.gov/MedicalDevices/Saf …
otices/ucm633960.htm