Critical flaw lets hackers control lifesaving devices implanted inside patients

Enlarge / An X-ray showing an cardio defibrillator implanted in a patient.

reader comments

37 with 32 posters participating

Share this story

The federal government on Thursday warned of a serious flaw in Medtronic cardio defibrillators that allows attackers to use radio communications to surreptitiously take full control of the lifesaving devices after they are implanted in a patient.

Defibrillators are small, surgically implanted devices that deliver electrical shocks to treat potentially fatal irregular heart rhythms. In recent decades, doctors have increasingly used radios to monitor and adjust the devices once they're implanted rather than using older, costlier, and more invasive means. An array of implanted cardio defibrillators made by Medtronic rely on two types of radio-based consoles for initial setup, periodic maintenance, and regular monitoring. Doctors use the company's CareLink Programmer in clinics, while patients use the MyCareLink Monitor in homes to regularly ensure the defibrillators are working properly.

No encryption, no authentication,

and a raft of other flaws

Researchers from security firm Clever Security discovered that the Conexus Radio Frequency Telemetry Protocol (Medtronic's proprietary means for the monitors to wirelessly connect to implanted devices) provides no encryption to secure communications. That makes it possible for attackers within radio range to eavesdrop on the communications. Even worse, the protocol has no means of authentication for legitimate devices to prove they are authorized to take control of the implanted devices. That lack of authentication, combined with a raft of other vulnerabilities, makes it possible for attackers within radio range to completely rewrite the defibrillator firmware, which is rarely seen in exploits that affect medical device vulnerabilities.

The researchers privately notified Medtronic of the critical vulnerability in January 2018. On Thursday, the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency issued an advisory that for the first time publicly disclosed the vulnerability:

> *Successful exploitation of these vulnerabilities may allow an attacker with adjacent short-range access to one of the affected products to interfere with, generate, modify, or intercept the radio frequency (RF) communication of the Medtronic proprietary Conexus telemetry system, potentially impacting product functionality and/or allowing access to transmitted sensitive data… 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.*

The advisory rated the severity at 9.3 out of a possible 10 points and said it required low skill to exploit. The notice went on to say that Medtronic has provided additional controls

to detect and respond to abuse of the Conexus protocol and continues to develop additional measures that will be deployed once they receive regulatory approval. In the meantime, the CISA notice advised patients to take the following precautions:

- *Maintain good physical control over home monitors and programmers*
- *Use only home monitors, programmers, and implantable devices obtained directly from your healthcare provider or a Medtronic representative to ensure integrity of the system*
- *Do not connect unapproved devices to home monitors and programmers through USB ports or other physical connections*
- *Only use programmers to connect and interact with implanted devices in physically controlled hospital and clinical environments*
- *Only use home monitors in private environments such as a home, apartment, or otherwise physically controlled environment*
- *Report any concerning behavior regarding these products to your healthcare provider or a Medtronic representative*

A proof-of-concept attack developed by the researchers was able to take control of the implanted devices in a manner previously unseen in most exploits affecting lifesaving medical devices. With physical access to either a MyCareLink or CareLink console, the researchers could make modifications that would pull patient names, physician names, and relevant phone numbers out of the device and make unauthorized and potentially fatal changes to the shocks the devices delivered. Even more stunning, the attack was able to read and rewrite all the firmware used to operate the implant.

With additional work, the researchers told Ars, they could have developed a custom hardware device that, when within range of an implanted defibrillator, could carry out the entire range of attacks performed by the modified MyCareLink and CareLink consoles. The researchers said the changes Medtronic has made to the consoles are designed to make it harder for them to wirelessly read and rewrite defibrillator firmware. They warned, however, that until wireless connections are encrypted and authenticated, the researchers don't believe there is any way to fully prevent attacks from either the consoles or custom hardware.

"The changes Medtronic has already made ATTEMPT to detect attacks," Peter Morgan, founder and principal at Clever Security, told Ars. "Without updates to the defibrillator firmware, it's not realistically possible to prevent. The changes are intended to detect malicious activity."

In an email, Medtronic representative Ryan Mathre wrote, in part:

> *There is a low practical risk of these vulnerabilities being exploited. To date, no cyberattack, privacy breach, or patient harm has been observed or associated with these issues.*
>
> *Even in the unlikely scenario that an unauthorized user may be able to access the wireless technology, that access does not equate to the ability to control or manipulate the settings of an implanted heart device.*
>
> *An unauthorized user would need comprehensive and specialized knowledge of medical devices, wireless telemetry, and electrophysiology to fully exploit these vulnerabilities in order to harm a specific patient. An unauthorized user would need to have a specific malicious intent, and would need to have specific knowledge of:*
>
> - *What device model is implanted in the patient*

- *What changes to the device would cause a patient harm*
- *What settings would need to be changed to alter the device function for that patient*
- *What telemetry command(s) are needed to implement that change*
- *When the patient's telemetry is active and susceptible to the unauthorized programming attempt*

> *Medtronic is developing a series of software updates to better secure the wireless communication affected by these issues. The first update is scheduled for later in 2019, subject to regulatory approvals.*
>
> *FDA and Medtronic recommend that patients and physicians continue to use devices and technology as prescribed and intended, as the benefits of remote monitoring outweigh the risks of exploiting these issues. To date, no cyberattack, privacy breach, or patient harm has been observed or associated with these issues.*
>
> *Even in the unlikely scenario that an unauthorized user may be able to access the wireless technology, that access does not equate to the ability to control or manipulate the settings of an implanted heart device. Fully exploiting these issues requires comprehensive and specialized knowledge of devices, wireless communication and electrophysiology.*

The attack described Thursday joins a raft of other vulnerabilities also discovered by Clever Security, some of which the DHS' CISA disclosed last June. The password that is required to gain root access to the custom version of Linux that powers the MyCareLink and CareLink monitors is an eight-character string that's protected by MD5, a hash algorithm that has long been deprecated for the protection of passwords. As a result, the researchers were able to crack the password in 30 seconds using a consumer-grade computer and a list of 14 million unique plain-text passwords exposed in a 2009 breach

of the RockYou gaming website.

For the attacks to succeed, defibrillators must be in a radio-frequency listen mode. Implanted devices go into this state when doctors are setting up or providing maintenance and when patients perform regular check-ins using the Carelink device. Periodically, the implanted devices enter this state on their own so they can check in with the Carelink monitor. The researchers said they didn't actively exploit the automatic listen mode, but they have confirmed it as a viable attack path.

With knowledge of the password and by physically connecting to a universal asynchronous receiver-transmitter debugging port that remained on the console's circuit board, the researchers were able to gain highly privileged root control of the console. They then exploited USB mass-storage capabilities that were enabled in the OS to make it possible to install new software on the monitors. Some of the software gave the consoles the ability to directly read and write firmware on the implanted devices.

The vulnerabilities are different from a series of flaws in the CareLink 2090 programmer disclosed in August. The lack of encrypted connections between the programmer and update servers and the absence of code-signing made it possible to infect the programmer with malware that could program the implants to deliver life-threatening shocks. Those vulnerabilities were discovered by researchers Billy Rios and Jonathan Butts.

Morgan, the Clever Security founder, said that his firm was already in the process of testing the Medtronic devices when he learned that a friend relied on one of them to treat a serious heart condition.

"Since our friend had this device implanted, there was a visceral sense of duty to ensure that the vulnerability gets

patched with the utmost care for anyone affected by the vulnerability," Morgan said. "It encouraged a patient tenacity throughout the disclosure process and really made things hit home. The friend still has the device. Hopefully he's a little bit safer than when we started."

https://arstechnica.com/?p=1478167