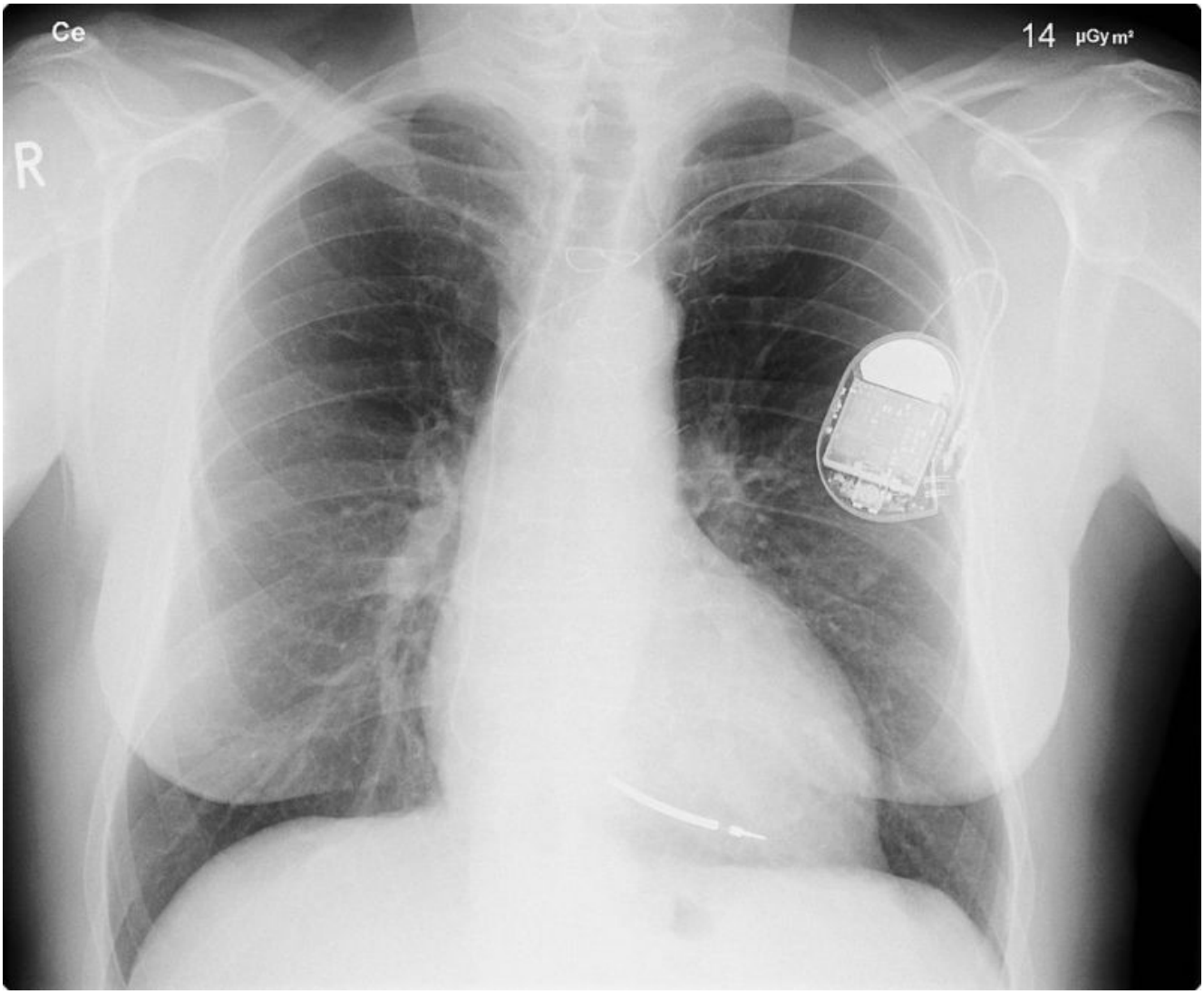
Critical flaw lets hackers control lifesaving devices implanted inside patients



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

Multiple Vulnerabilities Patched in PuTTY and LibSSH2

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/aGRh-BCgaAU/multiple-vulnerabilities-patched-putty-and-libssh2

Facebook Pays Big Bounty for DoS Flaw in Fizz TLS Library

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/tEE6DVFyCfQ/facebook-pays-big-bounty-dos-flaw-fizz-tls-library

---

Many Vulnerabilities Found in Oracle’s Java Card Technology

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/DoYpIOrcX-o/many-vulnerabilities-found-oracles-java-card-technology

---

Schneider Electric Working on Patch for Flaw in Triconex TriStation Emulator

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/Tt0FmnXqI5Y/schneider-electric-working-patch-flaw-triconex-tristation-emulator

Apple, Oracle, VMware Software Hacked at Pwn2Own 2019

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/z1i4G2jeW8k/apple-oracle-vmware-software-hacked-pwn2own-2019

Google Photos Flaw Allowed Hackers to Track Users

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/PKmTXD8whjs/google-photos-flaw-allowed-hackers-track-users

---

How a wireless keyboard lets hackers take full control of connected computers



reader comments

59 with 41 posters participating

Share this story

There’s a critical vulnerability in a model of Fujitsu wireless keyboard that makes it easy for hackers to take full control of connected computers, security researchers warned on Friday. Anyone using the keyboard model should strongly consider replacing it immediately.

The Fujitsu Wireless Keyboard Set LX901 uses a proprietary 2.4 GHz radio communication protocol called WirelessUSB LP from Cypress Semiconductor. While the keyboard and mouse send input that’s protected with the time-tested Advanced Encryption Standard, the USB dongle that accepts the input accepts unencrypted packets as well, as long as they’re in the proper

format.

Researchers with the Germany-based penetration-testing firm SySS developed a proof-of-concept attack that exploits the insecure design. Using a small hardware device, they are able to send commands to vulnerable Fujitsu keyboard receiver dongles that are within range. As the video below demonstrates, the researchers were able to send input of their choice that's automatically funneled to the connected computer.

[embedded content]
Fujitsu LX901 Keystroke Injection Attack PoC

But wait … it gets worse

In an advisory published Friday, the researchers warned they can combined this injection exploit with a replay attack SySS disclosed in 2016. The earlier exploit allows attackers to record encrypted keystrokes the wireless keyboard sends to the USB dongle receiver. Attackers can then launch a replay attack, in which hackers send the recorded data to the receiver. In the event hackers record the keystrokes the rightful computer owner uses to unlock the machine, the attackers can later use them to gain access when the computer is locked and unattended.

The attacks can be carried out by anyone who is within range of an affected keyboard set and takes the time to build the hardware that exploits the replay and injection flaws. Normally, that distance is about 30 feet, but the use of special antennas could extend that range. That leaves open the possibility of attacks from hackers in nearby offices or homes.

Friday's SySS advisory said that there is currently no known fix for the vulnerabilities. It said company researchers privately reported the vulnerability to Fujitsu. The

disclosure timeline is:

> *2018-10-19: Vulnerability reported to manufacturer*
> *2018-10-22: Fujitsu confirms receipt of security advisory*
> *2018-10-25: Fujitsu asks for more information about the reported security issue*
> *2018-10-26: Provided more information concerning the reported security vulnerability to Fujitsu*
> *2018-10-29: Fujitsu asks for more information about the reported security issue and proof of attacks (replay and keystroke injection)*
> *2018-10-30: Clarified some misunderstandings concerning the replay (SYSS-2016-068) and the keystroke injection (SYSS-2018-033) vulnerabilities, provided source code of a developed PoC tool, and provided videos with proof-of-concept attacks exploiting these two security issues*
> *2019-03-15: Public release of security advisory*

Matthias Deeg, a SySS researcher, said there is no reliable way keyboard users can protect themselves against the vulnerabilities other than to ensure they are completely isolated from all other radio-based devices.

“The only protection I can think of is having an extensive control over the environment and the people where the keyboard is used,” he wrote in an email. “Using the keyboard in a radio-shielded place, for instance a basement, where no untrustworthy person can gain physical proximity and send any radio data packets to the USB receiver, should be quite secure. =).”

“But I do not recommend using this vulnerable keyboard in an environment with higher security demands,” he continued. “And I would advise not using it in exposed places where external attackers may come easily in the 2.4 GHz radio communication range of the wireless keyboard, for instance at service desks in stores, or in banks, or in train stations, or at airports.”

Attempts to reach Fujitsu representatives for comment weren’t immediately successful.

https://arstechnica.com/?p=1475021

Recently Patched WinRAR Flaw Exploited in APT Attacks

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/W9kDCMmpFCE/recently-patched-winrar-flaw-exploited-apt-attacks

---

Details of Actively Exploited Windows Flaw Made Public

[unable to retrieve full-text content]http://feedproxy.google.com/~r/Securityweek/~3/-zgnJRxjNNY/details-actively-exploited-windows-flaw-made-public