Medtronic Security Bulletin, 21 maart 2019
Conexus™ Telemetry en Monitoring Accessores

Medtronic heeft een bulletin naar buiten gebracht over de cyberveiligheid van bepaalde producten. Het bericht heeft betrekking op de draadloze technologie die wordt gebruikt bij sommige Medtronic-hartimplantaten, programmeerapparaten en thuismonitoren. Onderzoekers hebben mogelijke kwetsbaarheden ontdekt in bepaalde modellen van ICD's (implanteerbare cardioverter-defibrillatoren) en CRT-D's (implanteerbare cardiale resynchronisatietherapie / defibrillatorapparaten) en de technologie die wordt gebruikt voor de communicatie tussen die geïmplanteerde apparaten en klinische programmeerapparaten en thuismonitors. Dit heeft geen betrekking op pacemakers van Medtronic, instelbare hartbewakingsapparatuur of andere Medtronic-apparaten.

Medtronic voert beveiligingscontroles uit om te zoeken naar ongeoorloofde of ongebruikelijke activiteiten die verband kunnen houden met deze mogelijke kwetsbaarheden. Misbruik is alleen mogelijk onder specifieke omstandigheden;
• de verbinding moet zijn geactiveerd door een zorgverlener die zich in dezelfde kamer als de patiënt bevindt, bijvoorbeeld tijdens de implantatieprocedure of tijdens follow-upbezoeken in het ziekenhuis;
• de activeringstijden buiten het ziekenhuis moeten bekend zijn. Deze tijden zijn beperkt, verschillen per patiënt en zijn moeilijk te voorspellen door een onbevoegde gebruiker;
• zeer dicht bij een actief apparaat, monitor of programmeerapparaat zijn, namelijk op minder dan 6 meter afstand;
• een onbevoegd persoon moet kennis hebben van het apparaat model dat de patiënt geïmplanteerd heeft gekregen;
• een onbevoegd persoon moet kennis hebben van de veranderingen aan het apparaat die een patiënt zouden kunnen schaden;
• de instellingen die moeten worden gewijzigd om de apparaat functie voor die patiënt te wijzigen moeten bekend zijn;
• de telemetrieopdracht(-en) die nodig zijn om die wijziging te implementeren moeten bekend zijn.

Tot op heden is geen cyberaanval, inbreuk op de privacy of patiëntletsel waargenomen of in verband gebracht met deze problemen.

Medtronic ontwikkelt een reeks software-updates om de draadloze communicatie beter te beveiligen tegen deze mogelijke kwetsbaarheden. De eerste update is gepland voor later in 2019, onder voorbehoud van goedkeuringen door toezichthouders.

Medtronic en de FDA bevelen patiënten en artsen aan om apparaten en technologie te blijven gebruiken zoals voorgeschreven en bedoeld, omdat dit de meest efficiënte manier biedt om de apparaten en hartaandoeningen van patiënten te beheren

Artsen kunnen bij vragen terecht bij hun Medtronic contact persoon.
Patiënten die zich zorgen maken, kunnen dit bespreken met hun arts

SECURITY BULLETIN

March 21, 2019

Conexus™ Telemetry and Monitoring Accessories

Medtronic

Vulnerability Summary

External security researchers Peter Morgan of Clever Security; Dave Singelée and Bart Preneel of KU Leuven; Eduard Marin formerly of KU Leuven and currently with the University of Birmingham; Flavio D. Garcia; Tom Chothia of the University of Birmingham; and Rik Willems of University Hospital Gasthuisberg Leuven disclosed potential cybersecurity vulnerabilities in some Medtronic products. The vulnerabilities apply to the proprietary Medtronic Conexus™ radio frequency wireless telemetry protocol (referred to "Conexus telemetry" in this document) associated with some Medtronic ICDs (implantable cardioverter defibrillators) and CRT-Ds (cardiac resynchronization therapy defibrillators). A complete list of affected products is at the end of this document.

To date, no cyberattack, privacy breach, or patient harm has been observed or associated with these vulnerabilities.

Conexus telemetry is **not** used in Medtronic pacemakers (including those with Bluetooth wireless functionality). Additionally, CareLink Express monitors and the CareLink Encore programmers (Model 29901) used by some hospitals and clinics do not use Conexus telemetry.

Conexus telemetry allows Medtronic programmers and monitoring accessories to:

- Remotely transmit data from a patient's implanted cardiac device to a specified health care clinic (i.e. remote monitoring), including important operational and safety notifications.
- Display and print device information in real time for clinicians.
- Program device settings.

The vulnerabilities could allow an unauthorized individual (i.e. someone other than a health care professional) to access and potentially change the settings of an implantable device, home monitor or clinic programmer. Medtronic is conducting security checks to look for unauthorized or unusual activity that could be related to these vulnerabilities.

Taking advantage of these vulnerabilities in order to cause harm to a patient would require detailed knowledge of medical devices, wireless telemetry and electrophysiology. Exploitation is also more difficult because:

- During the implant procedure and in-clinic follow-up visits, Conexus telemetry must be activated by a health care professional who is in the same room as the patient
- Outside of the hospital/clinic activation times are limited, vary by patient, and are difficult to be predicted by an unauthorized user.
- An unauthorized individual would need to be close to an active device, monitor, or clinic programmer to take advantage of these vulnerabilities. Depending on the surrounding environment, the typical maximum communications range between an active device and a monitor or programmer does not exceed 6 meters (20 feet).

Mitigation
Medtronic is developing updates to mitigate these vulnerabilities. We will inform patients and physicians when they become available (subject to regulatory approvals).

Medtronic recommends 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. These benefits include earlier detection of arrhythmias, fewer hospital visits and improved survival rates.

Patients with concerns about these cybersecurity vulnerabilities should discuss these concerns with their physicians.

The complete advisory issued by ICS-CERT can be found here.

Affected Products
The following products use the affected Conexus telemetry impacted by this vulnerability:

Implantable Devices
Amplia MRI™ CRT-D, all models
Claria MRI™ CRT-D, all models
Compia MRI™ CRT-D, all models
Concerto™ CRT-D, all models
Concerto™ II CRT-D, all models
Consulta™ CRT-D, all models
Evera MRI™ ICD, all models
Evera™ ICD, all models
Maximo™ II CRT-D and ICD, all models
Mirro MRI™ ICD, all models
Nayamed ND ICD, all models
Primo MRI™ ICD, all models
Protecta™ CRT-D and ICD, all models
Secura™ ICD, all models

Programmers and Monitors
CareLink™ 2090 Programmer
CareLink™ Monitor, Model 2490C
MyCareLink Monitor, models 24950 and 24952

Virtuoso™ ICD, all models
Virtuoso™ II ICD, all models
Visia AF MRI™ ICD, all models
Visia AF™ ICD, all models
Viva™ CRT-D, all models

Q&A:

Q: Why did the FDA issue a safety alert about this issue?
A: Medtronic disclosed vulnerabilities related to the proprietary wireless communication technology (Conexus telemetry) associated with certain Medtronic ICDs and CRT-Ds and programmers. We have also shared guidelines to mitigate cybersecurity risks related to Conexus telemetry.

Q: What is the practical risk to a patient?
A: Even though an unauthorized user may be able to access the Conexus telemetry, that access does not mean the unauthorized user will have the ability to control or change the settings of an implanted heart device. Fully exploiting these vulnerabilities requires comprehensive and specialized knowledge of medical devices, wireless telemetry and electrophysiology. These vulnerabilities are not accessible from the Internet.

To date, neither a cyberattack nor patient harm has been observed or associated with these vulnerabilities.

Q: What should a patient do next?
A: Medtronic recommends that patients and physicians continue to use devices as prescribed and intended. The benefits of remote monitoring outweigh the practical risk that these vulnerabilities could be exploited. The following guidelines should be used to further reduce the risk of these vulnerabilities:

- Use only the remote monitor obtained directly from a healthcare provider or Medtronic. This helps to ensure integrity of the system.
- Continue to keep the remote monitor plugged in at all times.
    - The remote monitor must remain powered up to ensure any wireless CareAlerts™ programmed by the physician and/or any automatically scheduled remote transmissions occur.
- Maintain good physical control over the remote monitor.
- Report any concerning behavior regarding these products to a healthcare provider or to Medtronic.

Patients with concerns about these cybersecurity vulnerabilities should discuss these concerns with their physician.

Medtronic Contact Information

US: Medtronic Patient and Technical Services is available to answer questions Monday-Friday 7am – 6pm central time at 855-275-2717.

International: Contact your local Medtronic representative.