VEILIGHEIDSBERICHT

21 maart 2019

Conexus™-telemetrie en monitoringsaccessoires

Medtronic

Samenvatting kwetsbaarheid

Externe veiligheidsonderzoekers Peter Morgan van Clever Security; Dave Singelée en Bart Preneel van de Katholieke Universiteit (KU) Leuven; Eduard Marin van voorheen KU Leuven en momenteel de University of Birmingham; Flavio D. Garcia; Tom Chothia van de University of Birmingham; en Rik Willems van Universitair Ziekenhuis Leuven, campus Gasthuisberg, hebben potentiële kwetsbaarheden op het gebied van cyberveiligheid aan het licht gebracht in bepaalde producten van Medtronic. De kwetsbaarheden zijn van toepassing op het beschermde radiofrequente, draadloze Medtronic Conexus™-telemetrieprotocol (in dit document aangeduid als 'Conexus-telemetrie') dat betrekking heeft op bepaalde ICD's (implanteerbare cardioverter defibrillatoren) en CRT-D's (defibrillatoren voor cardiale resynchronisatietherapie) van Medtronic. Een volledige lijst met producten die het betreft, is te vinden aan het eind van dit document.

Tot op heden is er geen enkele cyberaanval, privacyschending of letsel aan patiënten waargenomen of geassocieerd met deze kwetsbaarheden.

Conexus-telemetrie wordt niet gebruikt in pacemakers van Medtronic (inclusief die met draadloze Bluetooth-functionaliteit). Daarnaast maken de CareLink Express-monitoren en de CareLink Encore-programmeerapparaten (Model 29901), die door bepaalde ziekenhuizen en klinieken gebruikt worden, ook geen gebruik van Conexus-telemetrie.

Conexus-telemetrie stelt programmeerapparaten en monitoringsaccessoires van Medtronic in staat om:

- op afstand gegevens te verzenden van een hartimplantaat naar een specifieke zorgkliniek (zogenaamde controle op afstand), inclusief belangrijke operationele en veiligheidsmeldingen;
- informatie van het hartimplantaat voor artsen in real-time te tonen en af te drukken;
- instellingen van het hartimplantaat te programmeren.

De kwetsbaarheden zouden een niet-gemachtigd persoon (d.w.z. iemand anders dan een zorgverlener) toegang kunnen geven tot de gegevens en de mogelijkheid om instellingen te veranderen van een hartimplantaat, een thuismonitor of klinisch programmeerapparaat. Medtronic voert veiligheidscontroles uit, om te zoeken naar ongeautoriseerde of ongewone activiteiten die gerelateerd zouden kunnen zijn aan deze kwetsbaarheden.

Misbruik van deze kwetsbaarheden met het doel om een patiënt letsel toe te brengen, vereist gedetailleerde kennis van medische hulpmiddelen, draadloze telemetrie en elektrofysiologie.

Misbruik is ook moeilijker omdat:

- tijdens de implantatieprocedure en de vervolgcontrolebezoeken in het ziekenhuis de Conexus-telemetrie moet worden geactiveerd door een zorgverlener die zich in dezelfde ruimte bevindt als de patiënt;
- de activatietijden buiten het ziekenhuis beperkt zijn, ze per patiënt verschillen en ze moeilijk te voorspellen zijn door een ongeautoriseerde gebruiker;
- een ongeautoriseerd persoon zich dicht bij een actief hulpmiddel, monitor of klinisch programmeerapparaat moet bevinden om deze kwetsbaarheden te kunnen misbruiken.
  Afhankelijk van de omgeving is het typische maximale communicatiebereik tussen een actief hulpmiddel en een monitor of programmeerapparaat niet meer dan 6 meter.

Beperking
Medtronic ontwikkelt updates om deze kwetsbaarheden te beperken. We zullen patiënten en artsen informeren zodra deze beschikbaar komen (onderhevig aan wettelijke goedkeuring).

Medtronic raadt patiënten en artsen aan deze hulpmiddelen te blijven gebruiken zoals voorgeschreven en bedoeld. De voordelen van controle op afstand wegen zwaarder dan het praktische risico dat deze kwetsbaarheden zouden kunnen worden misbruikt. Deze voordelen omvatten vroegere detectie van ritmestoornissen, minder ziekenhuisbezoeken en hogere overlevingspercentages.

Patiënten die zich zorgen maken over deze cyberveiligheidskwetsbaarheden, kunnen hun zorgen bespreken met hun arts.

Het complete advies van ICS-CERT kunt u hier vinden.

Producten die het betreft
De volgende producten maken gebruik van de Conexus-telemetrie die getroffen is door deze kwetsbaarheid:

Implanteerbare apparaten	**Programmeerapparaten en monitoren**
Amplia MRI™ CRT-D, alle modellen	CareLink™ 2090-programmeerapparaat
Claria MRI™ CRT-D, alle modellen	CareLink™-monitor, Model 2490C
Compia MRI™ CRT-D, alle modellen	MyCareLink-monitor, Modellen 24950 en 24952
Concerto™ CRT-D, alle modellen	
Concerto™ II CRT-D, alle modellen	
Consulta™ CRT-D, alle modellen	
Evera MRI™ ICD, alle modellen	
Evera™ ICD, alle modellen	
Maximo™ II CRT-D en ICD, alle modellen	
Mirro MRI™ ICD, alle modellen	
Nayamed ND ICD, alle modellen	
Primo MRI™ ICD, alle modellen	
Protecta™ CRT-D en ICD, alle modellen	
Secura™ ICD, alle modellen	
Virtuoso™ ICD, alle modellen	
Virtuoso™ II ICD, alle modellen	
Visia AF MRI™ ICD, alle modellen	
Visia AF™ ICD, alle modellen	
Viva™ CRT-D, alle modellen	

Veelgestelde vragen:

V: Waarom heeft de FDA een veiligheidswaarschuwing afgegeven over dit probleem?
A: Medtronic heeft kwetsbaarheden bekendgemaakt met betrekking tot de beschermde draadloze communicatietechnologie (Conexus-telemetrie) die geassocieerd is met bepaalde ICD's, CRT-defibrillatoren en programmeerapparaten van Medtronic. We hebben ook richtlijnen gedeeld om de cyberbeveiligingsrisico's met betrekking tot Conexus-telemetrie te beperken.

V: Wat is het praktische risico voor een patiënt?
A: Alhoewel een ongeautoriseerde gebruiker toegang zou kunnen krijgen tot de Conexus-telemetrie, betekent die toegang niet dat de ongeautoriseerde gebruiker het hartimplantaat kan beïnvloeden of de instellingen ervan kan veranderen. Misbruik maken van deze kwetsbaarheden vereist uitgebreide en gespecialiseerde kennis over medische hulpmiddelen, draadloze telemetrie en elektrofysiologie. Deze kwetsbaarheden zijn niet toegankelijk via internet.

Tot op heden is er geen enkele cyberaanval of letsel aan een patiënt waargenomen of geassocieerd met deze kwetsbaarheden.

V: Wat moet een patiënt nu doen?
A: Medtronic raadt aan dat patiënten en artsen de hulpmiddelen blijven gebruiken zoals voorgeschreven en bedoeld. De voordelen van controle op afstand wegen zwaarder dan het praktische risico dat deze kwetsbaarheden zouden kunnen worden misbruikt. De volgende richtlijnen moeten gebruikt worden om het risico van deze kwetsbaarheden verder te reduceren:

- Alleen gebruikmaken van de monitor die u rechtstreeks van een zorgverlener of Medtronic heeft ontvangen. Dit helpt de integriteit van het systeem te waarborgen.
- De monitor continu aangesloten houden.
    - De monitor moet aan blijven staan om te verzekeren dat draadloze CareAlerts™ die door de arts geprogrammeerd zijn en/of automatische geplande verzendingen op afstand blijven plaatsvinden.
- Goede fysieke controle over de monitor bewaren.
- Elke zorgelijke gedraging met betrekking tot deze producten melden aan een zorgverlener of Medtronic.

Patiënten die zich zorgen maken over deze cyberveiligheidskwetsbaarheden, kunnen hun zorgen bespreken met hun arts.

Contactinformatie Medtronic:

Voor nadere informatie kunt u contact opnemen met PR-manager Nicole Velthuis, +316 20629845.