BULLETIN DE SECURITE

21Mars 2019

Télémetrie Conexus™ et accessoires de surveillance

Medtronic

Description de la vulnérabilité

Des chercheurs externes en sécurité, Peter Morgan de Clever Security, Dave Singelée et Bart Preneel de KU Leuven, Eduard Marin anciennement à KU Leuven et actuellement à l'Université de Birmingham, Flavio D. Garcia, Tom Chothia de l'Université de Birmingham et Rik Willems de l'University Hospital Gasthuisberg Leuvenont ont identifié des vulnérabilités de cybersécurité pour certains produits Medtronic. Celles-ci concernent le protocole de télémétrie sans fil Conexus™ (appelé "télémétrie Conexus" dans le présent document) associé à certains défibrillateurs et CRT-D (défibrillateurs de resynchronisation cardiaque) de Medtronic. La liste complète des produits concernés se trouve à la fin du présent document.

À ce jour, aucune cyberattaque, atteinte à la vie privée ou préjudice causé aux patients n'a été observé ou associé à ces vulnérabilités.

La télémétrie Conexus **n'est pas utilisée** dans les stimulateurs cardiaques de Medtronic (notamment ceux dotés de la fonctionnalité sans fil Bluetooth). De plus, les moniteurs CareLink Express et les programmateurs CareLink Encore (modèle 29901) utilisés par certains hôpitaux et cliniques n'utilisent pas la télémétrie Conexus.

La télémétrie Conexus permet aux programmateurs et aux moniteurs Carelink de :

- Transmettre à distance les données du dispositif cardiaque implanté à un patient vers son centre de suivi (télésurveillance), y compris des notifications importantes opérationnelles et/ou relative à la sécurité.
- Afficher et imprimer en temps réel les informations relatives à l'appareil pour les cliniciens.
- Programmer les paramètres de fonctionnement de l'appareil

Les vulnérabilités pourraient permettre à une personne non autorisée (c.-à-d. quelqu'un d'autre qu'un professionnel de la santé) d'accéder aux paramètres d'un dispositif implantable, d'un moniteur à domicile ou d'un programmeur clinique et de les modifier éventuellement. Medtronic effectue des contrôles de sécurité pour déceler toute activité non autorisée ou inhabituelle qui pourrait être liée à ces vulnérabilités.

Tirer parti de ces vulnérabilités pour causer du tort à un patient nécessiterait une connaissance approfondie des dispositifs médicaux, de la télémétrie sans fil et de l'électrophysiologie. Leur exploitation est difficile pour les raisons suivantes :

- Pendant l'implantation et les visites de suivi en clinique, la télémétrie Conexus doit être activée par un professionnel de la santé qui se trouve dans la même pièce que le patient.
- En dehors de l'hôpital/clinique, les temps d'activation sont limités, varient selon le patient et sont difficiles à prévoir par un utilisateur non autorisé.
- Une personne non autorisée devrait se trouver à proximité d'un dispositif actif, d'un moniteur ou d'un programmeur clinique pour tirer parti de ces vulnérabilités. Selon l'environnement, la portée de communication maximale typique entre un dispositif actif et un moniteur ou un programmateur ne dépasse pas 6 mètres.

Gestion des risques :

Medtronic développe des mises à jour logicielles pour atténuer ces vulnérabilités. Nous informerons les patients et les médecins dès qu'ils seront disponibles (sous réserve des approbations réglementaires).

Medtronic recommande aux patients et aux médecins de continuer à utiliser ces dispositifs comme prescrit et prévu. Les avantages de la télésurveillance l'emportent sur le risque pratique que ces vulnérabilités puissent être exploitées. Ces avantages comprennent la détection plus précoce des arythmies, la réduction du nombre de visites à l'hôpital et l'amélioration des taux de survie.

Les patients qui s'inquiètent de ces vulnérabilités en matière de cybersécurité devraient en discuter avec leur médecin.

Le bulletin complet publié par ICS-CERT est disponible sur : https://ics-cert.us-cert.gov/advisories

Produits concernés
Les produits suivants utilisent la télémétrie Conexus affectée par cette vulnérabilité :

Dispositifs implantables
Amplia MRI™ CRT-D, tous les modèles
Claria MRI™ CRT-D, tous les modèles
Compia MRI™ CRT-D, tous les modèles
Concerto™ CRT-D, tous les modèles
Concerto™ II CRT-D, tous les modèles
Consulta™ CRT-D, tous les modèles
Evera MRI™ ICD, tous les modèles
Evera™ ICD, tous les modèles
Maximo™ II CRT-D et ICD, tous les modèles
Mirro MRI™ ICD, tous les modèles
Nayamed ND ICD, tous les modèles
Primo MRI™ ICD, tous les modèles
Protecta™ CRT-D et ICD, tous les modèles
Secura™ ICD, tous les modèles
Virtuoso™ ICD, tous les modèles
Virtuoso™ II ICD, tous les modèles
Visia AF MRI™ ICD, tous les modèles
Visia AF™ ICD, tous les modèles
Viva™ CRT-D, tous les modèles

Programmateurs et Moniteurs
Programmateur CareLink™ 2090
Moniteur CareLink™, modèle 2490C
Moniteur MyCareLink™, modèles 24950 et 24952

Questions / réponses :

Q : Pourquoi la FDA a-t-elle émis une alerte de sécurité à ce sujet ?
R : Medtronic a révélé des vulnérabilités liées à la technologie de communication sans fil (télémétrie Conexus) associée à certains DAI, CRT-D et programmeurs de Medtronic. Nous avons également partagé des lignes de conduite pour limiter les risques de cybersécurité liés à la télémétrie Conexus.

Q : Quel est le risque pratique pour un patient ?
R : Même si un utilisateur non autorisé peut avoir accès à la télémétrie Conexus, cet accès ne signifie pas que cet utilisateur non autorisé aura la possibilité de contrôler ou de modifier les paramètres d'un dispositif cardiaque implanté. Pour exploiter pleinement ces vulnérabilités, il faut des connaissances approfondies et spécialisées sur les dispositifs médicaux, la télémétrie sans fil et l'électrophysiologie. Ces vulnérabilités ne sont pas accessibles depuis Internet.

Jusqu'à présent, aucune cyberattaque ni aucun préjudice pour les patients n'a été observé ou associé à ces vulnérabilités.

Q : Que doit-on recommander aux patients ?
R : Medtronic recommande aux patients et aux médecins de continuer à utiliser les dispositifs comme prescrit et prévu. Les avantages de la télésurveillance l'emportent sur le risque pratique que ces vulnérabilités puissent être exploitées. Les lignes de conduite suivantes peuvent être suivies pour limiter le risque lié à ces vulnérabilités :

- N'utilisez que le moniteur obtenu directement d'un fournisseur de soins de santé ou de Medtronic. Cela permet d'assurer l'intégrité du système.
- Continuez de brancher le moniteur à distance en tout temps.
    - Le moniteur à distance doit rester sous tension pour s'assurer que toute transmission sans fil CareAlerts™ programmée par le médecin et/ou toute transmission à distance programmée automatiquement, ait bien lieu.
- Gardez un bon contrôle physique sur le moniteur à distance.
- Signalez tout comportement préoccupant concernant ces produits à un fournisseur de soins de santé ou à Medtronic.

Les patients qui s'inquiètent de ces vulnérabilités en matière de cybersécurité doivent en faire part à leur médecin.

N'hésitez pas à contacter votre représentant commercial pour tout complément d'information.