URGENT FIELD SAFETY NOTICE - Urgente veiligheidsinformatie

Informatie over op cyberbeveiliging gerichte update voor Accent™/ Anthem™-, Accent MRI™/ Accent ST™- en Assurity™/ Allure™ en Assurity MRI™ hulpmiddelen

28 Augustus 2017

Geachte heer/mevrouw,

Hierbij brengen we u op de hoogte van de beschikbaarheid van nieuwe firmware (een soort software) voor pacemakers. De nieuwe firmwareversie is bedoeld ter beperking van het risico op onbevoegde toegang tot onze pacemakers die via radiofrequentie (RF) communiceren (te weten de Accent™/ Anthem™, Accent MRI™/ Accent ST™ , Assurity™/ Allure™ en Assurity MRI™). Deze firmware-update biedt een extra beveiligingslaag tegen onbevoegde toegang tot deze hulpmiddelen, waarmee het risico van een succesvolle cyberaanval verder wordt beperkt.

Deze nieuwe versie wordt vrijgegeven na lokale goedkeuring door de autoriteiten en maakt deel uit van de geplande updates die zijn begonnen met de verbeteringen van de Merlin@home™-software v8.2.2 in januari 2017. De update omvat een nieuwe softwareversie voor Merlin™-programmeerapparaten (versie 23.1.2). Deze versie omvat gegevenscodering, patches voor het besturingssysteem, en schakelt bepaalde functies voor netwerkconnectiviteit uit.

Onderstaande informatie is bedoeld om de zwakke plek in de cyberbeveiliging, de firmware-update en de daarmee samenhangende voordelen en risico's voor zorgprofessionals en patiënten inzichtelijk te maken.

Beschrijving van de zwakke plek in de cyberbeveiliging en de daarmee samenhangende risico's

We hebben geen meldingen ontvangen van inbreuk op een hulpmiddel gerelateerd aan de zwakke plekken in de cyberbeveiliging van de geïmplanteerde hulpmiddelen waar dit bericht betrekking op heeft. Gezien het lage risico voor patiënten kan implantatie van hulpmiddelen met de huidige firmware door blijven gaan totdat op lokaal niveau goedkeuring van de autoriteiten is verkregen voor de nieuwe firmware. Volgens het Amerikaanse Ministerie van Binnenlandse Veiligheid (Department of Homeland Security) zou een inbreuk op de beveiliging van deze hulpmiddelen een uiterst complexe aanval vergen, zou bij een geslaagde aanval een onbevoegd persoon (d.w.z. een aanvaller in de buurt) toegang kunnen krijgen en het geïmplanteerde hulpmiddel via radiofrequentiecommunicatie (RF) commando's kunnen geven. Verder zouden die onbevoegde commando's instellingen kunnen veranderen (bijvoorbeeld stoppen met stimuleren) of de functionaliteit van het hulpmiddel kunnen beïnvloeden. [1]

[1] Zie ICS-CERT-kennisgeving ICSMA-17-XXX-0X ABBOTT LABORATORIES PACEMAKER VULNERABILITIES

Bijzonderheden over firmware-update en daarmee samenhangende risico's

Met firmware wordt de specifieke software bedoeld die op de hardware van de pacemaker staat. Het firmware-updateproces neemt ongeveer drie minuten in beslag en gedurende die tijd werkt het hulpmiddel in de backup-modus (VVI-stimulering met 67 slagen per minuut); essentiële, levensreddende functies blijven beschikbaar. Na afronding van de update keert het hulpmiddel terug naar de instellingen van voor de update.

Op basis van onze ervaring met eerdere firmware-updates, is er sprake van een klein aantal storingen als gevolg van de update (zoals bij elke software-update). Mogelijke risico's zijn onder andere:

- herladen van de voorgaande firmwareversie door een onvolledige update (0,161% van de gevallen);
- verlies van de op dat moment geprogrammeerde instellingen (0,023% van de gevallen);
- volledige uitval van functionaliteit (0,003% van de gevallen);
- verlies van diagnostische gegevens (niet gemeld).

Aanbevelingen voor patiëntbegeleiding

Profylactische vervanging van de betrokken hulpmiddelen wordt niet aanbevolen.

Hoewel uw professionele oordeel over de noodzaak van een firmware-update bij een bepaalde patiënt uiteraard vooropstaat, bevelen wij in samenspraak met onze medische adviesraad voor cyberbeveiliging het volgende aan:

1. Bespreek de risico's en voordelen van de zwakke plekken in de cyberbeveiliging en de bijbehorende firmware-update met uw patiënten tijdens hun eerstvolgende reguliere controle. In dat kader is het belangrijk om patiënt specifieke zaken mee te wegen (zoals pacemakerafhankelijkheid, de leeftijd van het hulpmiddel en de voorkeuren van de patiënt) en om hem/haar de 'Kennisgeving voor patiënten' te verstrekken.

2. Stel vast of de update nodig is gezien het risico ervan voor de patiënt. Indien u de firmware-update nodig acht, installeert u deze update volgens de instructies op het programmeerapparaat (en onderstaande aanwijzingen).

3. Voor pacemakerafhankelijke patiënten moet worden overwogen of de firmware-update kan worden uitgevoerd in een instelling waar mogelijkheid tot tijdelijke stimulatie en wisseling van de pacemakergenerator voorhanden is, in verband met het als zeer gering ingeschatte risico van het mislukken van de firmware-update.

Firmware-updateproces

Tijdens het firmware-updateproces wordt het hulpmiddel tijdelijk in de backup-modus gezet. Wij raden zorgprofessionals aan om de geprogrammeerde instellingen voorafgaand aan de update vast te leggen voor het geval deze na de update niet correct worden hersteld. Het updateproces verloopt als volgt:

- **Abbott-vertegenwoordigers werken het Merlin™-programmeerapparaat bij met nieuwe software**. De nieuwe software van het programmeerapparaat zorgt ervoor dat de firmware-update wordt uitgevoerd.

- **Het programmeerapparaat geeft een melding bij het uitlezen van een hulpmiddel**. Na het updaten van het programmeerapparaat en nadat het hulpmiddel is uitgelezen, geeft het programmeerapparaat een waarschuwing over een beschikbare update. Voordat de waarschuwing wordt weergegeven, kunnen geprogrammeerde instellingen worden afgedrukt om de tot dan toe gebruikte instellingen vast te leggen.

- **Op het programmeerapparaat wordt een volgende schermwaarschuwing weergegeven**. De arts volgt de instructies op het scherm om verder te gaan.

- **De arts selecteert de firmware-update voor cyberbeveiliging**. Het programmeerapparaat downloadt de nieuwe firmware naar het hulpmiddel van de patiënt. De update kan niet op afstand worden uitgevoerd.

- **Het downloaden neemt circa drie minuten in beslag**. De telemetrische wand moet boven het hulpmiddel worden gehouden totdat de firmware-update voltooid is.

- **Na de update moet worden gecontroleerd of het hulpmiddel naar behoren functioneert en niet in de backup-modus blijft staan.** Controleer of de instellingen van het hulpmiddel na de update zijn hersteld naar de instellingen die daarvóór in gebruik waren, en controleer of de diagnostische gegevens nog beschikbaar zijn. Als van één van beide geen sprake is, herhaal dan het proces en/of neem contact op met de technische ondersteuningsdienst van Abbott.

Als u vragen hebt over de firmware-update voor cyberbeveiliging kunt u contact opnemen met uw Abbott-vertegenwoordiger of ons speciale telefoonnummer voor technische ondersteuning bellen: +46 8474 4147 (EU). Aanvullende informatie, waaronder de kennisgeving voor patiënten, vindt u op www.sjm.com/notices.

Abbott blijft beveiligingsupdates uitbrengen voor de hulpmiddelen in ons portfolio in het kader van onze voortdurende inzet voor veilige en effectieve producten voor onze patiënten. Uw feedback is belangrijk voor ons, dus als u vragen of opmerkingen hebt over deze update, neemt u dan vooral contact op met uw Abbott-vertegenwoordiger.

Met vriendelijke groet,

Susan Jezior Slane
Divisional Vice President, Global Quality Systems and Compliance
Cardiovascular and Neuromodulation