Abbott

VIGTIG MEDDELELSE OM MEDICINSK UDSTYR

Oplysninger om cybersikkerhed Opdatering til enhederne Accent™/ Anthem™, Accent MRI™/ Accent ST™, Assurity™/ Allure™ og Assurity MRI™

28. august 2017

Til lægen

Vi gør opmærksom på, at der fås en ny pacemaker-firmware (en slags software), der er beregnet til at løse problemet med faren for uautoriseret adgang til de af vores pacemakere, der bruger radiofrekvent (RF) kommunikation (f.eks. Accent™/ Anthem™, Accent MRI™/ Accent ST™, Assurity™/ Allure™ og Assurity MRI™). Denne firmwareopdatering har et yderligere lag af sikkerhed mod uautoriseret adgang til disse enheder, og reducerer muligheden for at et cyberangreb lykkes.

Denne udgave bliver lanceret efter en lokal godkendelse af myndighederne og er en del af de planlagte opdateringer, der begyndte i januar 2017 med en forbedring af Merlin@home™ v8.2.2 softwaren. Opdateringen indeholder en softwareudgave til Merlin™-programmere (version 23.1.2), der ud over firmwareopdateringen inkluderer datakryptering, programrettelser til operativsystemet og deaktivering af netværkforbindelsesfunktioner.

Nedenstående oplysninger er beregnet til at hjælpe læger og patienter med at forstå cybersikkerhedens vulnerabilitet, firmwareopdateringen og de medfølgende fordele og risici.

<u>Beskrivelse af cybersikkerhedens vulnerabilitet og forbundne risici</u>

Vi har ikke modtaget rapporter om problemer med enheder, der skyldes cybersikkerhedens vulnerabilitet i de implanterede enheder, der er påvirket af denne meddelelse, og fortsat implantation af den aktuelle firmware, indtil der er opnået en lokal lovmæssig godkendelse af, at den nye firmware er egnet til patienter, der har behov for pacemakerbehandling. I henhold til United States Department of Homeland Security vil en kompromittering af disse enheders sikkerhed kræve et yderst avanceret angreb, hvis angrebet skulle lykkes, kunne en uautoriseret person (f.eks. en angrebsmand i nærheden) få adgang og udstede kommandoer til den implanterede medicinske enhed vha. radiofrekvente (RF) overførselsegenskaber, og disse uautoriserede kommandoer kunne ændre enhedens indstillinger (f.eks. standse pacing) eller påvirke implantatets funktion. [1]

[1] Der henvises til ICS-CERT Communication ICSMA-17-XXX-0X ABBOTT LABORATORIES Pacemaker VULNERABILITIES

Detaljer om firmwareopdateringen og forbundne risici

Firmware henviser til den specielle form for software, der er indbygget i pacemakerenhedens hardware. Firmwarens opdateringsproces tager ca. 3 minutter, og i løbet af denne tid virker enheden i backup-modus (VVI pacing ved 67 bpm), men essentielle livreddende funktioner er stadig tilgængelige. Efter opdateringen vender enheden tilbage til indstillingerne før opdateringen.

Baseret på vores erfaringer med tidligere firmwareopdateringer er der som ved alle softwareopdateringer en lav forekomst af funktionsfejl, der skyldes opdateringen. Disse risici (og deres forekomster) inkluderer, men er ikke begrænset til:

- genindlæsning af tidligere firmwareversioner pga. ufuldstændig opdatering (0,161%),
- tab af aktuelt programmerede enhedsindstillinger (0,023%),
- fuldstændigt tab af enheden funktion (0,003%) og
- tab af diagnostiske data (ikke rapporteret).

Anbefalinger vedrørende patientbehandling

Profylaktisk udskiftning af påvirkede enheder kan ikke anbefales.

Selv om det ikke er ment som en erstatning for professionel vurdering om hvorvidt firmwwareopdateringen er tilrådelig for en specifik patient, anbefaler vi sammen med vores Cyber Security Medical Advisory Board følgende:

1. Diskuter cybersikkerhedens vulnerabilitet og den tilsvarende firmwareopdaterings risici og fordele med patienten ved det næste planlagte besøg. Som en del af denne diskussion er det vigtigt at overveje problemer, der er specifikke for patienten, som for eksempel pacemakerafhængighed, enhedens alder og patientens præferencer og at give dem "Patient Communication".

2. Bestem om opdateringen er hensigtsmæssig i betragtning af risikoen for patienten ved en opdatering. Hvis det vurderes at være hensigtsmæssigt, installeres firmwareopdateringen i henhold til anvisningerne på programmeren (og angivet herunder).

3. Til pacingafhængige patienter skal det, på grund af en lille risiko for fejlfunktion efter firmwareopdateringen, overvejes at udføre firmwarens cybersikkerhedsopdatering på et sted, hvor en midlertidig pacing og pacemaker ICD-ændring er til rådighed.

Opdateringsproces for firmware

I løbet af enhedens opdateringsproces for firmware placeres den midlertidigt i backup-modus. Det anbefales, at klinikere registrerer de programmerede enhedsindstillinger i tilfælde af, at de ikke gendannes korrekt efter opdateringen. Opdateringsprocessen foregår således:

- **Abbott-repræsentanter vil opdatere Merlin™-programmeren med nyt software**: Det nye programmersoftware giver mulighed for at opdatere enhedens firmware.

- **PCS'en viser en prompt, når en enhed er interrogeret**: Når PCS'en er opdateret, og enheden er interrogeret, giver progammeren en meddelelse, om at en opdatering er

tilgængelig. Før meddelelsen vises, kan enhedens programmerede parametre udskrives som en registrering af indstillingerne før opdateringen.

- **En follow-up-prompt på skærmen vises på PCS'en**: Lægen skal følge anvisningerne på skærmen for at fortsætte.

- **Lægen vælger firmwareopdateringen for cybersikkerhed**: PCS'en downloader den nye firmware til patienten enhed. Opdatering af firmware til cybersikkerhed kan ikke fjernbetjenes.

- **Download til enheden burde være færdig i løbet af ca. tre minutter**: Telemetrihovedet skal blive over enheden, indtil firmwareopdateringen er færdig.

- **Efter opdateringen kontrolleres det, at enheden fungerer korrekt og ikke befinder sig i backup-modus:** Efter opdateringen kontrolles det, at enhedens parametre er gendannet til indstillingerne før opdateringen, og det bekræftes, at de diagnostiske data stadig findes. Hvis noget af dette ikke sker, gentages processen og/eller Abbotts tekniske support kontaktes.

I tilfælde af spørgsmål vedrørende firmwarens cybersikkerhedsopdatering kontaktes en Abbott-repræsentant eller vores dertil indrettede tekniske kundesupports hotline på +46-8474-4147 (EU). Yderligere materialer inkl. Patient Communication findes på www.sjm.com/notice.

Som en del af vores vedvarende engagement i et design, der er forsvarligt, effektivt og sikkert, vil Abbott fortsætte med at lave sikkerhedsopdateringer til enhederne i vores porteføljе. Deres feedback er vigtigt for os, så kontakt venligst en Abbott-repræsentant, hvis De har spørgsmål eller kommentarer til denne opdatering.

Med venlig hilsen

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