Abbott

AVVISO URGENTE DI SICUREZZA DI CAMPO

Informazione sull'Aggiornamento della Sicurezza Informatica (Cybersecurity) per i dispositivi Accent™/Anthem™, Accent MRI™/Accent ST™ Assurity™/Allure™ e Assurity™ MRI™

28 Agosto 2017

Egregio Dottore,

Con la presente intendiamo comunicarLe la disponibilità di un nuovo firmware (un tipo di software) del pacemaker destinato a risolvere i rischi di accesso non autorizzato ai nostri pacemaker che utilizzano comunicazioni in radio frequenza (RF) (ad esempio Accent™/Anthem™, Accent MRI™/Accent ST™ e Assurity™/Allure™ e Assurity MRI™). Questo aggiornamento del firmware fornisce un ulteriore livello di protezione contro l'accesso non autorizzato a questi dispositivi e riduce ulteriormente la probabilità di un attacco efficace alla cybersecurity.

Questa versione verrà introdotta a seguito dell'approvazione regolatoria locale ed è parte degli aggiornamenti pianificati che hanno avuto inizio a Gennaio 2017 con i miglioramenti del software v8.2.2 del dispositivo Merlin@home™. L'aggiornamento contiene il rilascio di un software per i programmatori Merlin™ (versione 23.1.2), che include la crittografia dei dati, patch del sistema operativo e la disattivazione delle funzionalità di connettività di rete in aggiunta all'aggiornamento del firmware.

Le informazioni fornite di seguito intendono aiutare i medici e i pazienti a comprendere la vulnerabilità della Sicurezza Informatica (cybersecurity), l'aggiornamento del firmware e i relativi benefici e rischi.

Descrizione della Vulnerabilità della Cybersecurity e Rischi Associati

Non abbiamo ricevuto alcuna segnalazione di compromissione di dispositivi correlata alla vulnerabilità della cybersecurity nei dispositivi impiantati e impattati da questa comunicazione e continuare ad impiantare dispositivi con l'attuale firmware per i pazienti che necessitano della terapia del pacemaker, in attesa dell'approvazione regolatoria, è appropriato. Secondo il Department of Homeland Security degli Stati Uniti compromettere la sicurezza di questi dispositivi richiederebbe un attacco molto complesso. Se ci fosse un attacco efficace, un individuo non autorizzato (ad esempio un aggressore nelle vicinanze) potrebbe accedere e impostare parametri nel dispositivo medico impiantato attraverso la funzionalità di trasmissione in radiofrequenza (RF) e, quei parametri non autorizzati, potrebbero modificare le impostazioni del dispositivo (ad esempio, arrestare il pacing) o avere impatto sulla funzionalità del dispositivo stesso. [1]

[1] Far riferiemento alla Comunicazione ICS-CERT ICSMA-17-241-0X Abbott Laboratories Accent/Anthem Accent MRI Assurity/Allure and Assurity MRI Pacemaker Vulnerabilities

Aggiornamento del Firmware e Rischi Associati

Il Firmware si riferisce a un particolare tipo di software incorporato nell'hardware del pacemaker. Il processo di aggiornamento del firmware richiede circa 3 minuti per essere completato e, durante questo periodo, il dispositivo funzionerà in modalità di back-up (pacing VVI a 67 bpm) e le funzioni essenziali e sostenibili rimarranno disponibili. Al termine dell'aggiornamento il dispositivo tornerà alle sue impostazioni di pre-aggiornamento.

In base alle nostre precedenti esperienze di aggiornamenti del firmware, come con qualsiasi aggiornamento software, vi è un'incidenza molto bassa di malfunzionamento derivante dall'aggiornamento stesso. Questi rischi (e la relativa incidenza associata) includono, ma non sono limitati a:

- ricarica della versione precedente del firmware a causa di un aggiornamento incompleto (incidenza 0,161%),
- perdita delle impostazioni programmate del dispositivo (incidenza 0,023%),
- completa perdita di funzionalità del dispositivo (incidenza 0,003%) e
- perdita di dati diagnostici (incidenza non riportata).

Raccomandazioni per la Gestione dei Pazienti

La sostituzione profilattica del dispositivo coinvolto non è raccomandata.

Sebbene ciò non sia destinato a sostituire il Suo giudizio professionale sul fatto che l'aggiornamento del firmware sia consigliabile per un particolare paziente, noi, insieme al nostro Cyber Security Medical Advisory Board, consigliamo quanto segue:

1. Discutere i rischi e i benefici delle vulnerabilità della Cybersecurity e l'aggiornamento firmware associato con i Suoi pazienti in occasione della prossima visita di controllo pianificata. Come parte di questa discussione, è importante considerare le questioni specifiche del paziente come la dipendenza dal pacemaker, l'età del dispositivo e la preferenza del paziente. Fornire loro la "Comunicazione per il Paziente".

2. Determinare se l'aggiornamento sia appropriato dati i rischi per il paziente derivanti dall'aggiornamento. Se ritenuto appropriato, installare l'aggiornamento del firmware seguendo le istruzioni sul programmatore (ed elencate di seguito).

3. Per i pazienti pacemaker-dipendenti, considerare di eseguire l'aggiornamento del firmware in una struttura in cui sia possibile fornire la stimolazione temporanea e la sostituzione tempestiva del pacemaker a causa del rischio stimato molto basso di malfunzionamenti a seguito dell'aggiornamento del firmware.

Processo di Aggiornamento del Firmware

Durante il processo di aggiornamento del firmware il dispositivo verrà temporaneamente impostato in modalità di back up. I medici sono invitati a registrare le impostazioni programmate del dispositivo prima dell'aggiornamento nel caso in cui non vengano ripristinate correttamente dopo l'aggiornamento. Il processo per l'aggiornamento è il seguente:

- **Il Rappresentante Abbott aggiorna il programmatore Merlin™ con il nuovo software**: il nuovo software del programmatore permetterà al firmware del dispositivo di essere aggiornato.

- **Il programmatore fornisce un messaggio quando un dispositivo viene interrogato**: dopo che il programmatore è stato aggiornato e il dispositivo interrogato, il programmatore avviserà che l'aggiornamento è disponibile. Prima di visualizzare l'avviso, i parametri programmati del dispositivo possono essere stampati come documentazione dell'impostazione pre-aggiornamento.

- **Un messaggio di follow up viene visualizzato sullo schermo del programmatore**: il medico dovrà seguire le istruzioni sul monitor per continuare.

- **Il medico seleziona l'aggiornamento del firmware per la Cybersecurity**: il programmatore scaricherà il nuovo firmware nel dispositivo del paziente. L'aggiornamento del firmware della cybersecurity non può essere eseguito da remoto.

- **Il download nel dispositivo si dovrebbe completare in circa tre minuti**: la sonda della telemetria deve rimanere sul dispositivo fino al completamento dell'aggiornamento del firmware.

- **Dopo l'aggiornamento, verificare che il dispositivo funzioni correttamente e non in modalità di back-up:** controllare che i parametri del dispositivo siano ripristinati alle impostazioni pre-aggiornamento e confermare che i dati diagnostici siano ancora presenti. Se una di queste condizioni non si verifica, ripetere il processo e/o contattare il Supporto Tecnico Abbott.

In caso di domande sull'aggiornamento firmware relativo alla cybersecurity, può contattare il Suo Rappresentante Abbott o il nostro Supporto Tecnico dedicato al numero +46-8474-4147 (EU). Il materiale aggiuntivo, inclusa la "Comunicazione per il Paziente", può essere trovata nel sito www.sjm.com/notices.

Abbott continuerà a implementare aggiornamenti relativi alla sicurezza sui dispositivi del nostro portafoglio prodotti come parte del nostro impegno costante a progettare prodotti sicuri, efficaci e affidabili per i nostri pazienti. Il Suo feedback è importante, per questo motivo contatti il Suo rappresentante Abbott in caso di domande o commenti relativi a questo aggiornamento.

Cordialmente,

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