



WICHTIGE INFORMATION ZU EINEM MEDIZINPRODUKT

Informationen zu einem Cybersicherheits-Update für die folgenden Produkte: Accent™ / Anthem™, Accent MRI™ / Accent ST™ und Assurity™ / Allure™

28 August, 2017

Sehr geehrte Frau Doktor,
Sehr geehrter Herr Doktor,

wir möchten Sie darauf hinweisen, dass eine neue Herzschrittmacher-Firmware (eine bestimmte Art von Software) verfügbar ist, die dem Risiko eines unbefugten Zugriffs auf unsere Herzschrittmacher mit Radiofrequenz- (RF-) Funktion (Accent™ / Anthem™, Accent MRI™ / Accent ST™ und Assurity™ / Allure™) begegnen soll. Das Firmware-Update bietet eine zusätzliche Sicherheitsebene gegen unbefugte Zugriffe auf diese Geräte, die das Potenzial eines erfolgreichen Angriffs auf deren Cybersicherheit weiter reduziert.

Die Firmware wird nach Genehmigung durch die zuständigen Aufsichtsbehörden eingeführt und ist Teil der planmäßigen Updates, die mit den Verbesserungen der Merlin@home™ Software v8.2.2 im April 2017 begonnen haben. Neben dem Firmware-Update enthält dieses Update eine Software-Version für das Merlin™-Programmiergerät (Version 23.1.2), die eine Datenverschlüsselung, Betriebssystem-Patches und Deaktivierung von Netzwerkkonnektivitätsfunktionen beinhaltet.

Die folgenden Informationen sollen Ärzten und Patienten dabei helfen, Schwachstellen bei der Cybersicherheit, das Firmware-Update als solches und die damit verbundenen Nutzen und Risiken zu verstehen.

Beschreibung der Schwachstellen bei der Cybersicherheit und verbundene Risiken

Uns liegen keine Berichte über eine Gefährdung oder Beeinträchtigung aufgrund von Schwachstellen bei der Cybersicherheit bei den von dieser Mitteilung betroffenen implantierten Geräten vor. Die weitere Implantation von Schrittmachern mit der aktuellen Firmware bis zur Zulassung der neuen Firmware vor Ort stellt ein niedriges Risiko für den Patienten dar. Laut dem US-Ministerium für Innere Sicherheit (Department of Homeland Security) würde eine Beeinträchtigung der Sicherheit dieser Geräte einen hochgradig komplexen Angriff voraussetzen. Im Falle eines erfolgreichen Angriffs könnte eine unberechtigte Person (d.h. ein in der Nähe befindlicher Angreifer) Zugang zum Medizinprodukt erhalten und über die Radiofrequenz-gesteuerte (RF) Datenübertragungsfunktion Befehle an das implantierte Gerät geben. Diese nicht

autorisierten Befehle könnten dann zu Veränderungen bei den Geräteeinstellungen führen (z. B. Stopp der Stimulation) bzw. Gerätefunktionen beeinträchtigen.^[1]

Einzelheiten zum Firmware-Update und verbundene Risiken

Firmware bezeichnet die besondere Art von Software, die in die Hardware des Herzschrittmachers eingebettet ist. Das Firmware-Update dauert ca. 3 Minuten, und während dieser Zeit arbeitet das Gerät im Back-up-Modus (VVI-Stimulation bei 67 bpm) und wesentliche, lebenswichtige Funktionen bleiben verfügbar. Nach Beendigung des Updates kehrt das Gerät zu den vor dem Update eingestellten Werten zurück.

Anhand unserer bisherigen Erfahrungen mit Firmware-Updates können wir sagen, dass, wie bei jedem Software-Update, der Prozentsatz Update-bezogener Probleme äußerst niedrig ist. Zu diesen Risiken (prozentuale Anteile in Klammern) zählen unter anderem:

- erneutes Laden der vorherigen Firmware-Version wegen Unvollständigkeit des Updates (0,161 %),
- Verlust der aktuell programmierten Geräteeinstellungen (0,023 %),
- vollständiger Verlust der Gerätefunktion (0,003 %) und
- Verlust der Diagnostikdaten (wurde nicht berichtet).

Empfohlenes Patientenmanagement

Der prophylaktische Austausch betroffener Geräte wird nicht empfohlen.

Wenngleich wir damit Ihre professionelle Einschätzung, ob das Firmware-Update bei einem bestimmten Patienten ratsam ist, in keiner Weise ersetzen möchten, empfehlen wir gemeinsam mit unserem medizinischen Beirat für Cybersicherheit (Cyber Security Medical Advisory Board, CSMAB) folgendes:

1. Besprechen Sie die Risiken und Nutzen der Cybersecurity-Schwachstellen und der damit verbundenen Firmware-Aktualisierung mit Ihren Patienten beim nächsten planmäßigen Termin. Dabei sollten patientenspezifische Themen wie Herzschrittmacherabhängigkeit, Alter des Gerätes und Patientenpräferenz berücksichtigt und dem Patienten die „Mitteilung für Patienten“ ausgehändigt werden.
2. Entscheiden Sie, ob das Update-Risiko für den Patienten in einem angemessenen Verhältnis steht. Falls dies der Fall ist, installieren Sie das Firmware-Update, indem Sie den Anweisungen des Programmiergeräts (und den unten genannten Anweisungen) folgen.
3. Bei schrittmacherabhängigen Patienten sollte aufgrund der äußerst geringen Gefahr einer Fehlfunktion im Rahmen des Firmware-Updates die Durchführung des Cybersicherheits-Firmware-Updates in einer Einrichtung erwogen werden, in der ein temporäre Schrittmacherbehandlung verfügbar ist und ein Schrittmacheraustausch ohne weiteres durchgeführt werden kann.

^[1] Siehe hierzu die ICS-CERT-Mitteilung ICSMA-17-241-0X ABBOTT LABORATORIES SCHWACHSTELLEN bei Herzschrittmachern

Firmware Update

Während des Firmware-Updates wird das Gerät vorübergehend in einen Backup-Modus versetzt. Dem Arzt wird empfohlen, die programmierten Geräteeinstellungen vor dem Update aufzuzeichnen, für den Fall, dass sie nach dem Update nicht ordnungsgemäß wiederhergestellt werden. Der Update-Vorgang verläuft wie folgt:

- **Abbott-Repräsentanten werden das Merlin™ Programmiergerät mit der neuen Softwareversion aktualisieren:** Die neue Software des Programmiergeräts erlaubt dann das Update der Schrittmacher mit der neuen Firmware.
- **Bei der Geräteabfrage erscheint am Programmiergerät eine Meldung:** Nachdem das Update des Programmiergeräts durchgeführt und das Gerät abgefragt wurde, erscheint am Programmiergerät die Meldung, dass ein Update verfügbar ist. Vor Ansicht der Meldung können die im Gerät programmierten Parameter zur Protokollierung der Vor-Update-Einstellungen ausgedruckt werden.
- **Auf dem Bildschirm des Programmiergeräts erscheint eine Meldung:** Zum Fortfahren folgt der Arzt den Bildschirmanweisungen.
- **Der Arzt markiert das Cybersicherheits-Firmware-Update:** Das Programmiergerät lädt sodann die neue Firmware auf das Gerät des Patienten herunter. Das Cybersicherheits-Firmware-Update kann nicht telemetrisch durchgeführt werden.
- **Das Herunterladen auf das Gerät sollte in ca. drei Minuten abgeschlossen sein:** Der Telemetriekopf muss solange über dem Gerät aufgelegt bleiben, bis das Firmware-Update abgeschlossen ist.
- **Bestätigen Sie im Anschluss an das Update, dass das Gerät ordnungsgemäß funktioniert und sich nicht im Back-up-Modus befindet:** Prüfen Sie, ob die Geräteparameter nach der Aktualisierung auf die vor dem Update bestehenden Einstellungen zurückgesetzt wurden und bestätigen Sie, dass die Diagnostikdaten noch vorhanden sind. Ist dies nicht der Fall, wiederholen Sie bitte den Vorgang und/oder wenden Sie sich an den technischen Kundendienst von Abbott.

Falls Sie Fragen zum Cybersicherheits-Firmware-Update haben, wenden Sie sich gerne an Ihren Abbott-Repräsentanten oder an die spezielle Hotline des technischen Kundendienstes unter der Rufnummer +46-8474-4147 (EU). Zusätzliche Materialien einschließlich der „Mitteilung für Patienten“ finden Sie unter www.sjm.com/notices.

Im Rahmen unseres fortgesetzten Engagements für die Entwicklung sicherer und wirksamer Produkte für unsere Patienten wird Abbott auch weiterhin Sicherheits-Updates für in unserem Portfolio befindliche Produkte durchführen. Ihr Feedback ist uns wichtig. Wenden Sie sich daher bitte an Ihren Abbott-Repräsentanten, wenn Sie Fragen oder Anmerkungen zu diesem Update haben.

Mit freundlichen Grüßen