NOTA URGENTE DE SEGURIDAD

Información relativa a Actualización en Ciberseguridad de los dispositivos Accent™/ Anthem™, Accent MRI™/ Accent ST™, y Assurity™/ Allure™ y Assurity MRI™

28 de Agosto de 2017

Estimado Doctor,

Le informamos sobre la disponibilidad de un nuevo firmware (un tipo de software) para marcapasos destinado a abordar el riesgo de acceso no autorizado a nuestros marcapasos que utilizan comunicaciones de radiofrecuencia (RF) (Accent™/ Anthem™, Accent MRI™/ Accent ST™, and Assurity™/ Allure™ y Assurity MRI™). Esta actualización de firmware proporciona una medida de seguridad adicional contra el acceso no autorizado a dichos dispositivos y que reduce aún más un potencial ataque cibernético exitoso.

Esta versión se lanzará tras la aprobación regulatoria local y forma parte de las actualizaciones planificadas que comenzaron en Enero 2017 con las mejoras del software v8.2.2 del Merlin@home™. La actualización contiene una versión de software para los programadores Merlin™ (versión 23.1.2) que incluye encriptación de datos, parches de sistema operativo, y deshabilitación de las características de conectividad de red, además de la actualización del firmware.

La información proporcionada a continuación, tiene como objeto ayudar a los profesionales sanitarios y pacientes a comprender la vulnerabilidad de la seguridad cibernética, la actualización del firmware, junto a los beneficios y riesgos asociados.

Descripción de la Vulnerabilidad Cibernética y los Riesgos Asociados

No hemos recibido informes de dispositivos comprometidos en relación a la vulnerabilidad en ciberseguridad de dispositivos implantados afectados por esta comunicación y se continúa implantando con el firmware actual hasta que se obtenga aprobación regulatoria del nuevo firmware, ya que representa un bajo riesgo para el paciente. Según el Departamento de Seguridad Nacional de los Estados Unidos ("US Department of Homeland Security"), comprometer la seguridad de estos dispositivos requeriría un ataque altamente complejo. Si se produjera un ataque exitoso, un individuo no autorizado (por ejemplo, un atacante cercano), podría acceder y emitir órdenes al dispositivo médico implantado mediante su capacidad de transmisión por radiofrecuencia (RF), y aquellas ordenes no autorizadas podrían modificar los ajustes del dispositivo (por ejemplo, detener la estimulación) o la funcionalidad del dispositivo de afectado . [1]

[1] Refer to the ICS-CERT Communication ICSMA-17-241-0X Abbott Laboratories Accent/Anthem Accent MRI Assurity/Allure and Assurity MRI Pacemaker Vulnerabilities

Detalles de la Actualización del Firmware y Riesgos Asociados

El firmware hace referencia a un tipo particular de software que está incluido en el hardware del marcapasos. El proceso de actualización del firmware tarda aproximadamente 3 minutos en completarse, y durante este tiempo, el dispositivo funcionará en modo de seguridad (estimulación VVI a 67 lpm), y las características esenciales de soporte vital permanecen disponibles. Al finalizar la actualización, el dispositivo volverá a su configuración de antes de la actualización.

Basándonos en nuestra experiencia sobre actualización de firmware, al igual que en otra actualización de software; hay una tasa muy baja de mal funcionamiento debido a la actualización. Los riesgos (y sus tasas asociadas) incluyen pero no se limitan a:

- recarga de la versión anterior de firmware debido a una actualización incompleta (0,161%),
- pérdida de la configuración actual del dispositivo (0,023%),
- pérdida completa de la funcionalidad del dispositivo (0,003%), y
- pérdida de los datos de diagnóstico (no disponemos de reportes).

Recomendaciones para el Tratamiento de los Pacientes

No se recomienda la sustitución profiláctica de los dispositivos afectados.

Aunque no pretende servir como un sustituto de su juicio profesional en cuanto a si la actualización del firmware es recomendable para un paciente en particular; nosotros, junto con nuestro Comité Asesor Médico en Ciberseguridad, recomendamos lo siguiente:

1. Trate con sus pacientes en el próximo seguimiento rutinario programado, los riesgos y beneficios de las vulnerabilidades en ciberseguridad y la actualización del firmware asociado. Como parte de esta conversación, es importante, considerar temas específicos del paciente tales como la dependencia del marcapasos, la antigüedad del dispositivo, junto a las preferencias del paciente y facilitarle la "Comunicación al Paciente".

2. Determinar si la actualización es apropiada para el paciente, dado el riesgo de la actualización. Si se considera apropiado, instale esta actualización de firmware siguiendo las instrucciones del programador (se detallan a continuación).

3. Para pacientes dependientes de estimulación, considere realizar la actualización del firmware de ciberseguridad, en una instalación donde pueda disponer fácilmente de un marcapasos temporal y se pueda realizar un recambio del marcapasos; debido al muy bajo riesgo estimado de mal funcionamiento durante la actualización del firmware.

Proceso de Actualización del Firmware

Durante el proceso de actualización del firmware, el dispositivo se colocará temporalmente en modo de seguridad. Se aconseja a los médicos registrar los ajustes programados del dispositivo antes de la actualización, para el caso de que estos no se restauren correctamente después de la actualización. El proceso para la actualización es el siguiente:

- **Los representantes de Abbott actualizarán el programador Merlin™ con el nuevo software:** El nuevo software del programador permitirá que el firmware del dispositivo sea actualizado.

- **El Programador proporciona una indicación cuando se interroga un dispositivo:** Una vez que el programador ha sido actualizado, y el dispositivo ha sido interrogado, el programador proporcionara una alerta de que hay una actualización disponible. Antes de visualizar la alerta, los parámetros programados del dispositivo, pueden imprimirse y quedar como registro de los ajustes de antes de la actualización.

- **En el programador se visualizará un mensaje de seguimiento en la pantalla:** El médico seguirá las instrucciones dadas en la pantalla para continuar.

- **El medico selecciona la actualización del firmware de ciberseguridad:** El programador descargará el nuevo firmware al dispositivo del paciente. La actualización de firmware de ciberseguridad no se puede realizar de forma remota.

- **La descarga en el dispositivo debe completarse en aproximadamente tres minutos:** El cabezal de telemetría debe permanecer sobre el dispositivo hasta la finalización de la actualización del firmware.

- **Tras la actualización, verifique que el dispositivo funciona correctamente y no en modo de seguridad:** Tras la actualización, compruebe que los parámetros del dispositivo han sido restaurados a los ajustes de antes de la actualización y confirme que los datos de diagnóstico siguen estando presentes. Si alguno de estos no ocurriese, repita el proceso y/o contacte con el Servicio Técnico de Abbott.

Si necesita alguna aclaración sobre la actualización del firmware de ciberseguridad, póngase en contacto con su Representante de Abbott o en nuestro Servicio de Atención Técnica al Cliente en el teléfono +46-8474-4147 (para Europa). Materiales adicionales, incluida la comunicación con el paciente, se pueden encontrar en www.sjm.com/notices.

Abbott continuará realizando actualizaciones de seguridad en los dispositivos de nuestros productos como parte de nuestro compromiso continuo de diseñar productos seguros, efectivos y fiables para nuestros pacientes. Sus comentarios son importantes para nosotros, por ello, por favor, contacte con su representante de Abbott para cualquier aclaración o comentario relativo a dicha actualización.

Un cordial saludo,

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

Abbott

URGENT FIELD SAFETY NOTICE

Information About Cybersecurity Update for Accent™/ Anthem™, Accent MRI™/ Accent ST™, Assurity™/ Allure™ and Assurity MRI™ devices

28 August, 2017

Dear Doctor,

We are advising you of the availability of new pacemaker firmware (a type of software) that is intended to address the risk of unauthorized access to our pacemakers that utilize radio frequency (RF) communications (i.e., Accent™/ Anthem™, Accent MRI™/ Accent ST™, Assurity™/ Allure™ and Assurity MRI™). This firmware update provides an additional layer of security against unauthorized access to these devices that further reduces the potential for a successful cybersecurity attack.

This release will be launched following local regulatory approval and is part of planned updates that began with the January 2017 enhancements of the Merlin@home™ v8.2.2 software. The update contains a software release for Merlin™ programmers (version 23.1.2) including data encryption, operating system patches, and disabling network connectivity features in addition to the firmware update.

The information provided below is intended to assist clinicians and patients in understanding the cybersecurity vulnerability, the firmware update, and associated benefits and risks.

Description of Cybersecurity Vulnerability and Associated Risks

We have received no reports of device compromise related to the cybersecurity vulnerabilities in the implanted devices impacted by this communication and continued implant of the current firmware until the local regulatory approval of the new firmware is appropriate for patients who need pacemaker therapy. According to the US Department of Homeland Security, compromising the security of these devices would require a highly complex attack. If there were a successful attack an unauthorized individual (i.e., a nearby attacker) could gain access and issue commands to the implanted medical device through radio frequency (RF) transmission capability, and those unauthorized commands could modify device settings (e.g., stop pacing) or impact device functionality. [1]

[1] Refer to the ICS-CERT Communication ICSMA-17-241-0X Abbott Laboratories Accent/Anthem Accent MRI Assurity/Allure and Assurity MRI Pacemaker Vulnerabilities

Firmware Update Details and Associated Risks

Firmware refers to the particular kind of software that is embedded in the hardware of the pacemaker device. The firmware update process takes approximately 3 minutes to complete, and during this time, the device will operate in back-up mode (VVI pacing at 67 bpm), and essential, life-sustaining features remain available. At the completion of the update, the device will return to its pre-update settings.

Based on our previous firmware update experience, as with any software update, there is a very low rate of malfunction resulting from the update. These risks (and their associated rates) include but are not limited to:

- reloading of previous firmware version due to incomplete update (0.161%),
- loss of currently programmed device settings (0.023%),
- complete loss of device functionality (0.003%), and
- loss of diagnostic data (not reported).

Patient Management Recommendations

Prophylactic replacement of affected devices is not recommended.

While not intended to serve as a substitute for your professional judgment as to whether the firmware update is advisable for a particular patient, we, along with our Cyber Security Medical Advisory Board, recommend the following:

1. Discuss the risks and benefits of the cybersecurity vulnerabilities and associated firmware update with your patients at the next regularly scheduled visit. As part of this discussion, it is important to consider patient specific issues such as pacemaker dependence, age of device, and patient preference and provide them with the "Patient Communication".

2. Determine if the update is appropriate given the risk of update for the patient. If deemed appropriate, install this firmware update following the instructions on the programmer (and listed below).

3. For pacing dependent patients, consider performing the cybersecurity firmware update in a facility where temporary pacing and pacemaker generator change are readily available, due to the very small estimated risk of firmware update malfunction.

Firmware Update Process

During the firmware update process the device will be temporarily placed in a back-up mode. Clinicians are advised to record the programmed device settings before the update in case they are not properly restored after the update. The process for the update is as follows:

- **Abbott Representatives will update the Merlin™ programmer with new software**: The new programmer software will allow for device firmware to be updated.

- **The Programmer provides a prompt when a device is interrogated**: After the programmer has been updated and the device has been interrogated, the programmer will provide an alert that an update is available. Before viewing the alert, device programmed parameters may be printed out as a record of the pre-update settings.

- **A follow up on-screen prompt is displayed on programmer**: The physician will follow the on-screen instructions to continue.

- **The physician selects the cybersecurity firmware update**: The programmer will download new firmware to the patient's device. The cybersecurity firmware update cannot be delivered remotely.

- **The download to device should complete within approximately three minutes**: The telemetry wand must remain over the device until completion of the firmware update.

- **After the update, verify that the device is functioning appropriately and not in back-up mode:** Check that the device parameters have been restored to the pre-update settings after the update and confirm that diagnostic data are still present. If either of these does not occur, repeat the process and/or contact Abbott technical support.

If you have any questions about the cybersecurity firmware update you can contact your Abbott representative or our dedicated customer technical support hotline at +46-8474-4147 (EU). Additional materials, including the Patient Communication, can be found on www.sjm.com/notices.

Abbott will continue to make security updates across the devices within our portfolio as part of our ongoing commitment to design safe, effective and secure products for our patients. Your feedback is important to us, so please contact your Abbott representative with any questions or comments related to this update.

Sincerely,

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