



AVISO IMPORTANTE SOBRE DISPOSITIVO MÉDICO

Informação sobre Actualização de Cibersegurança para dispositivos Accent™/ Anthem™, Accent MRI™/ Accent ST™, Assurity™/ Allure™ e Assurity MRI™

28 de Agosto de 2017

Ex.mo Sr./a Dr./a,

Serve a presente para informar os médicos sobre a disponibilidade do novo firmware (um tipo de software) para pacemaker destinado a enfrentar o risco de acesso não autorizado aos nossos pacemakers que utilizam comunicações por rádiofrequência (ou seja, os dispositivos Accent™/ Anthem™, Accent MRI™/ Accent ST™ e Assurity™/ Allure™). Esta actualização do firmware fornece uma camada de segurança adicional contra um acesso não autorizado a estes dispositivos, que reduz ainda mais o potencial de um ataque de cibersegurança bem sucedido.

Esta versão será disponibilizada assim que obtivermos a aprovação regulamentar local e faz parte das actualizações planeadas que tiveram início com as melhorias introduzidas em Janeiro de 2017 no software Merlin@home™ v8.2.2. A actualização contém uma versão do software para os programadores Merlin™ (versão 23.1.2) incluindo encriptação de dados, patches para o sistema operativo, e funcionalidades de desactivação da rede, para além da actualização do firmware.

A informação fornecida abaixo destina-se a ajudar os médicos e os doentes a compreender a vulnerabilidade de cibersegurança, a actualização do firmware e os riscos e benefícios associados.

Descrição da Vulnerabilidade de Cibersegurança e dos Riscos Associados

Não recebemos qualquer notificação sobre dispositivos que sofram de um compromisso relacionado com vulnerabilidades de cibersegurança nos dispositivos implantados abrangidos por esta comunicação e a continuação da implantação do actual firmware até à aprovação regulamentar do novo firmware é adequada para doentes que necessitem de terapia por pacemaker. De acordo com o Departamento de Segurança Interna dos EUA, para comprometer a segurança destes dispositivos seria necessário um ataque extremamente complexo. Se tal ataque viesse a ocorrer, uma pessoa não autorizada (i.e., um atacante nas proximidades) poderia aceder ao dispositivo médico implantado através da capacidade de transmissão por rádiofrequência (RF), e emitir comandos não autorizados que poderiam alterar as suas definições (p. ex., uma paragem da estimulação) ou afectar a sua funcionalidade.^[1]

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

Detalhes da Actualização do Firmware e Riscos Associados

O firmware é um tipo especial de software que é incorporado no hardware do pacemaker. O processo de actualização do firmware demora aproximadamente 3 minutos a concluir e durante este tempo o dispositivo irá funcionar em modo de back-up (Estimulação VVI a 67 bpm), continuando a disponibilizar as funcionalidades essenciais de suporte de vida. Assim que a actualização ficar concluída, o dispositivo voltará às definições que estavam activas antes da actualização.

Com base na nossa experiência anterior em actualização de firmware, tal como em qualquer actualização de software, existe uma taxa muito reduzida de avaria em resultado da actualização. Estes riscos (e as taxas associadas) incluem, e não se limitam, designadamente:

- Recarregamento da versão anterior do firmware devido a uma actualização incompleta (0,161%),
- Perda das definições actualmente programadas do dispositivo (0,023%),
- Perda total da funcionalidade do dispositivo (0,003%), e
- Perda de dados de diagnóstico (não notificado).

Recomendações referentes à gestão de doentes

Não é recomendada a substituição profilática dos dispositivos afectados.

Não sendo um substituto do critério profissional do médico quanto à pertinência da actualização do firmware no caso de um doente específico, juntamente com a nossa Comissão de Aconselhamento Médico de Cibersegurança, recomendamos o seguinte:

1. Discutir com os doentes os riscos e os benefícios da actualização do firmware associada às vulnerabilidades de cibersegurança na sua próxima consulta de rotina. Como parte desta discussão, é importante ter em consideração aspectos específicos do doente, tal como a dependência do pacemaker, idade do dispositivo e a preferência do doente. O clínico deve igualmente fornecer a "Comunicação ao Doente".
2. Determinar se a actualização é apropriada, dado o risco que esta pode implicar para o doente. Se a actualização for considerada apropriada, o médico deve instalar a actualização do firmware seguindo as instruções do programador (vide lista abaixo).
3. Para os doentes dependentes de estimulação, o médico deve considerar a realização da actualização do firmware num local onde tenha imediatamente disponíveis um sistema de estimulação temporária e um gerador de pacemaker alternativo, em virtude do reduzido risco estimado de uma avaria durante a actualização do firmware.

Processo de Actualização do Firmware

Durante o processo de actualização do firmware, o dispositivo é colocado temporariamente em modo de back-up. Recomendamos aos médicos que registem as definições do dispositivo antes de implementarem a actualização, caso estas não sejam correctamente repostas após a actualização. O processo de actualização é o seguinte:

- **Os representantes da Abbott actualizarão o programador Merlin™ com o novo software:** O novo software do programador permitirá implementar a actualização do firmware no dispositivo.
- **O Programador emite uma mensagem de solicitação quando um dispositivo é interrogado:** Depois de o programador ter sido actualizado e o dispositivo ter sido interrogado, o programador emitirá um alerta em como está disponível uma actualização. Antes de visualizar o alerta, os parâmetros programados do dispositivo podem ser impressos, como forma de registo das definições activas antes da actualização.
- **É mostrada no ecrã do programador uma mensagem de solicitação de seguimento:** O clínico seguirá as instruções que aparecem no ecrã para poder continuar.
- **O médico selecciona a actualização de cibersegurança do firmware:** O programador descarregará o novo firmware para o dispositivo do doente. Não é possível efetuar remotamente a actualização de cibersegurança do firmware.
- **O descarregamento para o dispositivo deve demorar aproximadamente três minutos:** A cabeça de telemetria deve permanecer sobre o dispositivo até que esteja concluída a actualização do firmware.
- **Depois de concluir a actualização, o médico deve certificar-se que o dispositivo está a funcionar adequadamente e que não se encontra em modo de back-up.** Confirme que os parâmetros do dispositivo foram repostos de acordo com as definições activas antes da actualização, e confirme que os dados de diagnóstico continuam presentes. Caso não ocorra qualquer uma destas situações, repita o processo e/ou contacte o suporte técnico da Abbott.

Caso tenha alguma dúvida acerca da actualização de cibersegurança do firmware pode contactar o seu representante da Abbott ou ligar para linha directa de suporte técnico dedicada, através do número +46-8474-4147 (EU).

No nosso website www.sjm.com/notices pode encontrar informação adicional, incluindo a Comunicação ao Doente.

A Abbott continuará a realizar actualizações de segurança dos dispositivos comercializados pela marca como parte do seu compromisso contínuo de conceber produtos seguros e eficazes para os nossos doentes. O seu feedback é importante para nós. Contacte o seu representante da Abbott se tiver dúvidas ou questões relacionadas com esta actualização.

Com os melhores cumprimentos,



Susan Jezior Slane
Vice-presidente de Divisão, Global Quality Assurance and Compliance
Cardiovascular and Neuromodulation