



Insights

Implantable Cardiac Devices Raise Cyber-Security Concerns

January 30, 2017

By: Stephanie T. Eckerle and Stacy Walton Long

The FDA continues to monitor and assess potential cybersecurity vulnerabilities associated with radio frequency (“RF”) enabled implantable devices. The FDA recently reviewed St. Jude Medical’s Merlin@home Transmitter and software patch – an implantable cardiac device – to determine any cybersecurity risks. The FDA proposed recommendations for healthcare providers, patients, and caregivers who use this device to prevent exploitation of cybersecurity vulnerabilities associated with these type of medical devices.

Although there has been no reported cybersecurity attacks associated with St. Jude Medical’s Merlin@home Transmitter and software patch, the FDA has confirmed that cybersecurity vulnerabilities do exist with such medical devices of which the public should be made aware.

As these medical devices become more interconnected with the internet, healthcare providers’ networks, smartphones, etc., the risk of exploitation of cybersecurity vulnerabilities increases. The FDA has confirmed, by reviewing the St. Jude Medical’s Merlin@home Transmitter, that an unauthorized user may exploit vulnerabilities by gaining remote access to a patient’s RF-enabled medical device and altering the Merlin@home Transmitter. Such modifications could affect the “programming commands to the implanted device, which could result in rapid battery depletion and/or administration of inappropriate pacing or shocks.”[1]

To address these cybersecurity vulnerabilities and improve patient safety, St. Jude Medical developed a software patch for the Merlin@home Transmitter. The patch is now available and will be applied automatically to the Merlin@home Transmitter. The FDA has reviewed the software patch to determine if it addresses the cybersecurity vulnerabilities, the risk of exploitation, and reduces patient harm associated with such exploitation. The FDA has concluded that the health benefits to the patient from continued use of these devices outweigh the cybersecurity risks.

The FDA will continue to monitor and assess new information regarding potential cybersecurity risks associated with St. Jude Medical’s Merlin@home Transmitter and patch, as well as any other new RF-enabled implantable medical devices that are introduced to the market. Although these medical devices connected to communication networks may increase cybersecurity vulnerabilities, at the same time, these type of devices can offer safer and more convenient healthcare to patients.

Potential cybersecurity vulnerabilities in medical devices is an issue the FDA takes very seriously. The FDA has issued recommendations to manufactures of these medical devices to continue to test and monitor these devices, and report any cybersecurity vulnerabilities to the FDA. The FDA specifically sets forth the following recommendations for healthcare providers who use St. Jude Medical’s Merlin@home Transmitter and patch:



- Continue to conduct in-office follow-up, per normal routine, with patients who have an implantable cardiac device that is monitored using the Merlin@home Transmitter.
- Remind patients to keep their Merlin@home Transmitter connected as this will ensure that patients' devices receive the necessary patches and updates.
- Contact St. Jude Medical's Merlin@home customer service at 1-877-My-Merlin, or visit www.sjm.com/Merlindisclaimer icon for answers to questions and additional information regarding St. Jude Medical's implantable cardiac devices, or the Merlin@home Transmitter.[2]

Further, the FDA proposes the following recommendations for patients and caregivers who use St. Jude Medical's Merlin@home Transmitter and patch:

- Follow the labeling instructions provided with your Merlin@home Transmitter. Keeping your monitor connected as directed will ensure your monitor receives necessary updates and patches. Keep in mind that although all connected medical devices, including this one, carry certain risks, the FDA has determined that the benefits to patients from continued use of the device outweigh the risks.
- Consult with your physician(s) for routine care and follow-up. Your ongoing medical management should be individualized based on your medical history and clinical condition.
- Visit www.sjm.com/Merlindisclaimer icon, or contact St. Jude Medical's Merlin@home customer service at 1-877-My-Merlin for additional information, or if you have any questions or issues regarding your St. Jude Medical implantable cardiac device, or your Merlin@home Transmitter.
- Seek immediate medical attention if you have symptoms of lightheadedness, dizziness, loss of consciousness, chest pain, or severe shortness of breath.[3]

If you have any questions regarding this article or RF-enabled implantable medical devices, and potential cybersecurity risks associated with such devices, please contact Stephanie T. Eckerle or Stacy Walton Long.

[1] <http://www.fda.gov/Safety/MedWatch/SafetyInformation/SafetyAlertsforHumanMedicalProducts/ucm535979.htm>

[2] See n.1

[3] See n.1