Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication

Date Issued:

January 9, 2017

Audience:

- Patients with a radio frequency (RF)-enabled St. Jude Medical implantable cardiac device and corresponding Merlin@home Transmitter
- Caregivers of patients with an RF-enabled St. Jude Medical implantable cardiac device and corresponding Merlin@home Transmitter
- Cardiologists, electrophysiologists, cardiothoracic surgeons, and primary care physicians treating patients with heart failure or heart rhythm problems using an RF-enabled St. Jude Medical implantable cardiac device and corresponding Merlin@home Transmitter

Medical Specialties:

Cardiac Electrophysiology, Cardiology, Cardiothoracic Surgery, Heart Failure

Device:

St. Jude Medical implantable cardiac devices (pacemakers, defibrillators, and resynchronization devices) provide pacing for slow heart rhythms and electrical shock or pacing to stop dangerously fast heart rhythms. These cardiac devices are implanted under the skin in the upper chest area with connecting insulated wires called "leads" that go into the heart. A patient may need an implantable cardiac device if their heartbeat is too slow (bradycardia), too fast (tachycardia), or needs coordination to treat heart failure.

The St. Jude Medical Merlin@home Transmitter uses a home monitor that transmits and receives RF signals used to wirelessly connect to the patient's implanted cardiac device and read the data stored on the device. The transmitter, located in the patient's home, sends the patient's data to his or her physician(s) via the Merlin.net Patient Care Network using a continuous landline, cellular, or wireless ("wi-fi") Internet connection.

When connected to the Merlin.net Patient Care Network, patients can direct their data to be uploaded or it can be automatically uploaded. Uploading a patient's data to the Merlin.net Patient Care Network allows his or her physician(s) to more frequently receive, assess, and monitor the patient's implantable cardiac device's function, which supports patient safety, and may reduce the number of in-office visits a patient needs.

Purpose:

The FDA is providing information and recommendations regarding St. Jude Medical's radio frequency (RF)-enabled implantable cardiac devices and Merlin@home Transmitter to reduce the risk of patient harm due to cybersecurity vulnerabilities.

For the purposes of this safety communication, cybersecurity—also sometimes referred to as "information security"—focuses on protecting patients' medical devices and their associated computers, networks, programs, and data from unintended or unauthorized access, change, or destruction.

Summary of Problem and Scope:

Many medical devices—including St. Jude Medical's implantable cardiac devices—contain configurable embedded computer systems that can be vulnerable to cybersecurity intrusions and exploits. As medical devices become increasingly interconnected via the Internet, hospital networks, other medical devices, and smartphones, there is an increased risk of exploitation of cybersecurity vulnerabilities, some of which could affect how a medical device operates.

The FDA has reviewed information concerning potential cybersecurity vulnerabilities associated with St. Jude Medical's Merlin@home Transmitter and has confirmed that these vulnerabilities, if exploited, could allow an unauthorized user, i.e., someone other than the patient's physician, to remotely access a patient's RF-enabled implanted cardiac device by altering the Merlin@home Transmitter. The altered Merlin@home Transmitter could then be used to modify programming commands to the implanted device, which could result in rapid battery depletion and/or administration of inappropriate pacing or shocks.

There have been no reports of patient harm related to these cybersecurity vulnerabilities.

To improve patient safety, St. Jude Medical has developed and validated a software patch for the Merlin@home Transmitter that addresses and reduces the risk of specific cybersecurity vulnerabilities. The patch, which will be available beginning **January 9, 2017**, will be applied automatically to the Merlin@home Transmitter. Patients and patient caregivers only need to make sure their Merlin@home Transmitter remains plugged in and connected to the Merlin.net network to receive the patch.

The FDA has reviewed St. Jude Medical's software patch to ensure that it addresses the greatest risks posed by these cybersecurity vulnerabilities, and reduces the risk of exploitation and subsequent patient harm. The FDA conducted an assessment of the benefits and risks of using the Merlin@home Transmitter, and has determined that the health benefits to patients from continued use of the device outweigh the cybersecurity risks.

Recommendations for Health Care Providers:

- 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/Merlin (http://www.sjm.com/Merlin) (http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Disclaimers/default.htm)** for answers to questions and additional information regarding St. Jude Medical's implantable cardiac devices, or the Merlin@home Transmitter.

Recommendations for Patients and Caregivers:

- 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/Merlin (http://www.sjm.com/Merlin)** **(http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Disclaimers/default.htm)**, 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.

FDA Actions:

The FDA will continue to assess new information concerning the cybersecurity of St. Jude Medical's implantable cardiac devices and the Merlin@home Transmitter, and will keep the public informed if the FDA's recommendations change.

The FDA reminds patients, patient caregivers, and health care providers that any medical device connected to a communications network (e.g. wi-fi, public or home Internet) may have cybersecurity vulnerabilities that could be exploited by unauthorized users. The increased use of wireless technology and software in medical devices, however, can also often offer safer, more efficient, convenient and timely health care delivery.

The FDA will continue its work with manufacturers and health care delivery organizations—as well as security researchers and other government agencies—to develop and implement solutions to address cybersecurity issues throughout a device's total product lifecycle. The FDA takes reports of vulnerabilities in medical devices very seriously and has issued **recommendations to manufacturers (/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf)** for continued monitoring, reporting, and remediation of medical device cybersecurity vulnerabilities.

Reporting Problems to the FDA:

Prompt reporting of adverse events can help the FDA identify and better understand the risks related to the use of medical devices. If you suspect or experience a problem with these devices, we encourage you to file a voluntary report through **MedWatch, the FDA Safety Information and Adverse Event Reporting program (/Safety/MedWatch/HowToReport/default.htm)**. Health care personnel employed by facilities that are subject to the **FDA's user facility reporting requirements (/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/ReportingAdverseEvents/default.htm)** should follow the reporting procedures established by their facilities.

Additional Resources:

- **St. Jude Medical Press Release: *St. Jude Medical Announces Cybersecurity Updates* (January 9, 2017) (http://media.sjm.com/newsroom/news-releases/news-releases-details/2017/St-Jude-Medical-Announces-Cybersecurity-Updates/default.aspx)** **(http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Disclaimers/default.htm)**
- **Department of Homeland Security NCCIC/ICS-CERT Medical Device Advisory: St. Jude Merlin@home Transmitter Vulnerability (https://ics-cert.us-cert.gov/advisories/ICSMA-17-009-01)** **(http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Disclaimers/default.htm)**
- **St. Jude Medical's Merlin.net Patient Care Network (https://www.sjm.com/en/patients/arrhythmias/our-solutions/remote-monitoring/merlin-net-pcn)** **(http://www.fda.gov/AboutFDA/AboutThisWebsite/WebsitePolicies/Disclaimers/default.htm)**
- **FDA Final Guidance on Postmarket Management of Cybersecurity in Medical Devices (/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf)**

Contact Information: