Abbott: New pacemaker firmware update addresses vulnerabilities

1 September 2017, by Nancy Owano

Credit: Abbott

(Tech Xplore)—Regarding cybersecurity vulnerabilities identified in Abbott's (formerly St. Jude Medical's) implantable cardiac pacemakers, the US Food and Drug Administration issued a firmware update dated August 29.

Its intended audience was spelled out. They are patients with a radio frequency (RF)-enabled St. Jude Medical implantable pacemaker; relevant caregivers of patients with RF-enabled St. Jude Medical implantable cardiac pacemakers; and cardiologists, electrophysiologists, cardiothoracic surgeons and primary care physicians who have patients with heart failure or heart rhythm problems using RF-enabled St. Jude Medical implantable cardiac pacemakers.

The St. Jude Medical site also addressed a "Cybersecurity Update" on August 29:

"Abbott released an update to its implantable pacemakers as part of its ongoing commitment to continuously improve patient care. This planned update to pacemaker firmware (a kind of software) adds additional security protections designed to reduce the risk of unauthorized access to patients' pacemakers."

An August 29 press release from Abbott said, "The update contains a software release that includes data encryption, operating system patches, and the ability to disable network connectively features, in addition to the firmware update."

The Abbott press release also listed the products.

The St. Jude Medical site provided a link to a patient guide FAQ.

The devices—implanted under the skin with wires ("leads") going into the heart—are designed to provide pacing for slow or irregular heart rhythms.

The FDA update said that "This communication does NOT apply to any implantable cardiac defibrillators (ICDs) or to cardiac resynchronization ICDs (CRT-Ds)."

The FDA explained: "On August 23, 2017, the FDA approved a firmware update that is now available and is intended as a recall, specifically a corrective action, to reduce the risk of patient harm due to potential exploitation of cybersecurity vulnerabilities for certain Abbott (formerly St. Jude Medical) pacemakers."

Meanwhile, the official website of the Department of Homeland Security issued an August 29 advisory too, in which it stated "A third-party security research firm has verified that the new firmware version mitigates the identified vulnerabilities."

In the description of vulnerabilities, the DHS advisory said they could be exploited via an adjacent network. "Exploitability is dependent on an attacker being sufficiently close to the target pacemaker as to allow RF communications."

The firmware update became available as of August 29, so any pacemakers manufactured

beginning August 28 will already have the update pre-loaded in the device, in turn not requiring the update.

"A firmware is basically software for a hardware, and the update should be an easier fix for patients than undergoing surgery for a new, hack-proof device," said Natt Garun in *The Verge*.

As noted by a BBC report, the benefit of allowing pacemakers to send and receive data wirelessly is that patients can pair them with an at-home transmitter at home monitoring the devices as patients sleep, potentially alerting them to medical problems.

The firmware update requires an in-person patient visit with a health care provider, said the FDA; it cannot be done from home via Merlin.net. The DHS advisory also noted the firmware update can be applied to an implanted pacemaker via the Merlin PCS Programmer by a healthcare provider.

The FDA firmware update said that "After installing this update, any device attempting to communicate with the implanted pacemaker must provide authorization to do so. The Merlin Programmer and Merlin@home Transmitter will provide such authorization."

Also, the FDA firmware update recommended that patients and health care providers discuss risks and benefits of the cybersecurity vulnerabilities as well as this update to address vulnerabilities, at the next regularly scheduled visit.

Both the FDA and Abbott did not recommend prophylactic removal and replacement of affected devices.

The update involves a process taking about 3 minutes to complete with the device operating in backup mode. Life-sustaining features remain available. At completion, the device returns to its pre-update settings.

From the FDA firmware update communication: "St. Jude Medical has developed and validated this firmware update as a corrective action (recall) for all of their RF-enabled pacemaker devices, including cardiac resynchronization pacemakers. The FDA has approved St. Jude Medical's firmware update to ensure that it addresses these cybersecurity vulnerabilities, and reduces the risk of exploitation and subsequent patient harm."

Abbott on August 29 said it "notified physicians of updates to its implantable pacemakers and defibrillators as part of its ongoing commitment to continuously improve patient care."

More information:
www.fda.gov/MedicalDevices/Saf … otices/ucm573669.htm