UNITED STATES

PRIVACY AND SECURITY FANATIC

By Ms. Smith, CSO

SEP 4, 2017 10:04 AM PDT

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

NEWS

465,000 Abbott pacemakers vulnerable to hacking, need a firmware fix

The FDA and Homeland Security issued alerts about vulnerabilities in Abbott (formerly St. Jude Medical) pacemakers and a firmware update to close those security holes.

An acquaintance of mine told me he received a notification from his doctor about cybersecurity vulnerabilities in his pacemaker. He's not alone. The FDA issued an alert about security flaws in 465,000 pacemakers that use radio frequency communications and came from Abbott (formerly St. Jude Medical).

The "fix" is not a surgical replacement pacemaker, but a firmware update that takes about three minutes to complete and carries a "very low risk of update malfunction;" a very small percentage of people might experience a "complete loss of device functionality" during the firmware update. The patch covers St. Jude Medical's pacemakers: Accent, Anthem, Accent MRI, Accent ST, Assurity and Allure.

My acquaintance's doctor, who he swears has been very good to him in the past, said he could come in and have the firmware fix if he wanted to, but he suggested against it because if it wasn't much of an issue. Unlike some pacemaker patients, this dude works in IT and understands the impact described in the ICS-CERT advisory:

[Learn 8 pitfalls that undermine security program success and 12 tips for effectively presenting cybersecurity to the board. | Sign up for CSO newsletters.]

> *Successful exploitation of these vulnerabilities may allow a nearby attacker to gain unauthorized access to a pacemaker and issue commands, change settings, or otherwise interfere with the intended function of the pacemaker.*

The pacemaker vulnerabilities include improper authentication that can be compromised or bypassed, another flaw that could allow a nearby attacker to issue commands to drain the battery, as well as a flaw that allows sensitive patient information being transmitted without encryption.

The code to exploit the pacemakers reportedly is not floating around in the wild, but it seems unwise for any cardiologist to downplay the risks and discourage patients from coming in to get the firmware update. Perhaps not all understand why the firmware is important. After all, an Abbott press release noted that "an advisory issued by the U.S. Department of Homeland Security [said] compromising the security of these devices would require a highly complex set of circumstances."

Yet according to the letter Abbott sent doctors (pdf download), "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."

Now that Abbott has publicly admitted to the security vulnerabilities and released a firmware update, why blow it off? It took a long time, an ethical battle in the security community and a lot of heat to get to the point that a firmware fix being released.

What it took to get a pacemaker firmware fix

Let's rewind a bit for the big picture. A year ago, MedSec teamed up with short-selling firm Muddy Waters and publicly disclosed (pdf) remotely exploitable flaws found in St. Jude pacemakers and defibrillators. Shares of St. Jude immediately fell, despite St. Jude vehemently denying the "false and misleading" report. St. Jude also filed a lawsuit for defamation, as the security community argued ethics of the disclosure.

St. Jude disputed pretty much everything Muddy Waters and MedSec claimed, including that the implantable medical devices could be hacked — battery depleted — at a distance of 50 feet, saying the wireless range was about 7 feet.

In October 2016, MedSec released four videos demonstrating the attacks. St Jude blew off the "unverified claims." But then, cybersecurity firm Bishop Fox "replicated first-hand many of the attacks."

The Bishop Fox report (pdf) claimed, "The wireless protocol used for communication amongst St. Jude Medical cardiac devices has serious security vulnerabilities that make it possible to convert Merlin@home devices into weapons capable of disabling therapeutic care and delivering shocks to patients at distances of 10 feet, a range that could be extended using off-the-shelf parts to modify Merlinn@home units."

Let's flash forward to January 2017. After Abbott Laboratories acquired St. Jude Medical for close to $25 billion, the FDA issued an alert and Homeland Security's ICS-CERT issued an advisory about many of the cybersecurity vulnerabilities that MedSec and Muddy Waters had first publicly disclosed. To "improve patient safety," St. Jude released a patch for vulnerabilities it had previously denied.

Muddy Waters claimed the "fixes do not appear to address many of the larger problems, including the existence of a universal code that could allow hackers to control the implants."

Profits Over Patients pointed out, "Matthew Green, an assistant professor for computer science at Johns Hopkins University and a part of the Bishop Fox team, called one vulnerability 'probably the most impactful vulnerability I've ever seen.'"

Meanwhile, the lawsuit raged on.

Zip forward a few months to April when the FDA sent a warning letter that roasted Abbott for failing to address the vulnerabilities, including those first pointed out to St. Jude as far back as April 2014. Furthermore, the firm claimed there had been no deaths related to the battery depletion issue, even though the first death related to that flaw occurred in 2014.

Zoom forward to August 2017, and we're back where we started, with the FDA and the Department of Homeland Security warning about cybersecurity vulnerabilities in 465,000 pacemakers that need the newly released firmware patch. Oh, and I've not seen anything about the lawsuit being dropped.

This may be a first, but the FDA warned:

> *Many medical devices — including St. Jude Medical's implantable cardiac pacemakers — 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.*

More information about the pacemaker firmware patch

As for this firmware fix, you can input your device's model number to find out if it is subject to the battery depletion advisory. You can read the product advisories here, read the FDA notice here, and read the Department of Homeland Security's notice here.

Next read this

- *The 10 most powerful cybersecurity companies*
- *7 hot cybersecurity trends (and 2 going cold)*
- *The Apache Log4j vulnerabilities: A timeline*
- *Using the NIST Cybersecurity Framework to address organizational risk*
- *11 penetration testing tools the pros use*

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

Follow