Advisory (ICSMA-17-241-01)

Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities

Original release date: August 29, 2017

OVERVIEW

MedSec Holdings Ltd has identified vulnerabilities in Abbott Laboratories' (formerly St. Jude Medical) pacemakers. Abbott has produced a firmware patch to help mitigate the identified vulnerabilities in their pacemakers that utilize radio frequency (RF) communications. A third-party security research firm has verified that the new firmware version mitigates the identified vulnerabilities.

The Food and Drug Administration (FDA) released a safety communication on August 29, 2017, Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication, regarding the identified vulnerabilities and corresponding mitigation. In response, ICS-CERT is releasing this advisory to provide additional detail to patients and healthcare providers.

AFFECTED PRODUCTS

The following pacemakers manufactured prior to August 28, 2017, are affected:

- Accent/Anthem,
- Accent MRI,
- Assurity/Allure, and
- Assurity MRI.

IMPACT

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.

BACKGROUND

Abbott is a US-based company headquartered in Abbott Park, Illinois.

The affected pacemakers are implantable medical devices designed to deliver electrical pulses to correct a slow heartbeat or no heartbeat at all. According to Abbott, these pacemakers are deployed across the Healthcare and Public Health sector. Abbott indicates that these products are used worldwide; however, Accent and Anthem are no longer sold in the US.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IMPROPER AUTHENTICATION[a]

The pacemaker's authentication algorithm, which involves an authentication key and time stamp, can be compromised or bypassed, which may allow a nearby attacker to issue unauthorized commands to the pacemaker via RF communications.

CVE-2017-12712[b] has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).[c]

IMPROPER RESTRICTION OF POWER CONSUMPTION[d]

The pacemakers do not restrict or limit the number of correctly formatted "RF wake-up" commands that can be received, which may allow a nearby attacker to repeatedly send commands to reduce pacemaker battery life.

CVE-2017-12714[e] has been assigned to this vulnerability. A CVSS v3 base score of 5.3 has been assigned; the CVSS vector string is (AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).[f]

MISSING ENCRYPTION OF SENSITIVE DATA[g]

The Accent and Anthem pacemakers transmit unencrypted patient information via RF communications to programmers and home monitoring units. The Assurity and Allure pacemakers do not contain this vulnerability. Additionally, the Accent and Anthem pacemakers store the optional patient information without encryption; however, the Assurity and Allure pacemakers encrypt stored patient information.

CVE-2017-12716[h] has been assigned to this vulnerability. A CVSS v3 base score of 3.1 has been assigned; the CVSS vector string is (AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).[i]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities 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.

EXISTENCE OF EXPLOIT

Exploitation of vulnerabilities has been publicly demonstrated; however, exploit code is not publicly available.

DIFFICULTY

An attacker with high skill would be able to exploit these vulnerabilities.

MITIGATION

Abbott has developed a firmware update to help mitigate the identified vulnerabilities. The version numbers of the firmware update for each product family are as follows:

- Accent/Anthem, Version F0B.0E.7E,
- Accent MRI/Accent ST, Version F10.08.6C,
- Assurity/Allure, Version F14.07.80, and
- Assurity MRI, Version F17.01.49.

The pacemaker firmware update will implement "RF wake-up" protections and limit the commands that can be issued to pacemakers via RF communications. Additionally the updated pacemaker firmware will prevent unencrypted transmission of patient information (Accent and Anthem only). The firmware update can be applied to an implanted pacemaker via the Merlin PCS Programmer by a healthcare provider. It is recommended that healthcare providers discuss this update with their patients and carefully consider the potential risk of a cybersecurity attack along with the risk of performing a firmware update. Implementation of the firmware update is to be determined based on the physician's professional judgment and patient management considerations. Pacemakers manufactured beginning August 28, 2017, will have this update preloaded on devices.

Abbott states that firmware updates should be approached with caution. Like any software update, firmware updates can cause devices to malfunction. Potential risks include loss of device settings, the device going into back-up mode, reloading of the previous firmware due to a failed upgrade, loss of diagnostic data, and a complete loss of device functionality. The Abbott Cybersecurity Medical Advisory Board has reviewed this firmware update and the associated risk of performing the update in the context of potential cybersecurity risk.

While not intended to serve as a substitute for clinician judgment as to whether the firmware update is advisable for a particular patient, the Cybersecurity Medical Advisory Board recommends the following:

- Healthcare providers and patients should discuss the risk and benefits of the cybersecurity vulnerabilities and associated firmware update during the next regularly scheduled visit. As part of this discussion, it is important to consider patient-specific issues such as pacemaker dependence, age of device, patient preference, and provide patients with the "Patient Communication."
- Determine if the update is appropriate given the risk of update for the patient. If deemed appropriate, install this firmware update following the instructions provided by the manufacturer.
- For pacing dependent patients, consider performing the cybersecurity firmware update in a facility where temporary pacing and pacemaker generator change are readily available, due to the risk of firmware update malfunction.

Patients and healthcare providers with questions can call the dedicated hotline at 1-800-722-3774 (U.S.) or visit https://www.sjm.com/cyberupdate for more information.

The FDA issued a safety communication on August 29, 2017, Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication, is available at the following location:

https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm

---

a. CWE-287: Improper Authentication, http://cwe.mitre.org/data/definitions/287.html, web site last accessed August 29, 2017.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12712, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

c. CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S..., web site last accessed August 29, 2017.

d. CWE-920: Improper Restriction of Power Consumption, http://cwe.mitre.org/data/definitions/920.html, web site last accessed August 29, 2017.

e. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12714, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

f. CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S..., web site last accessed August 29, 2017.

g. CWE-311: Missing Encryption of Sensitive Data, http://cwe.mitre.org/data/definitions/311.html, web site last accessed August 29, 2017.

h. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12716, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory.

i. CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S..., web site last accessed August 29, 2017.

Contact Information

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu