2018-077: Abbott Laboratories Defibrillator vulnerabilities

CERT Australia is aware of vulnerabilities in the Abbott Laboratories' (formerly St. Jude Medical) Implantable Cardioverter Defibrillator (ICD) and Cardiac Resynchronization Therapy Defibrillator (CRT-D). These vulnerabilities could allow a nearby attacker to gain unauthorized access to an ICD to issue commands, change settings, or otherwise interfere with the intended function of the ICD.

Abbott has developed a firmware update to help mitigate the identified vulnerabilities. Noting that this is an implantable device, it is important that patients have a discussion with their healthcare provider to determine whether the update is appropriate for them. In some cases it may be determined that patient-specific issues create too great a risk for the update to be performed. Where deemed appropriate, the update should be installed following the instructions provided by the manufacturer, and in a medical facility where appropriate monitoring and external defibrillation are readily available.

AFFECTED PRODUCTS

The following ICDs and CRT-Ds manufactured and distributed prior to April 19, 2018, are affected:

- Current,
- Ellipse,
- Fortify Assura,
- Fortify,
- Promote Quadra,
- Promote,
- Quadra Assura MP,
- Quadra Assura,
- Unify Assura,
- Unify Quadra,
- Unify.

RECOMMENDATIONS

The affected ICDs and CRT-Ds are implantable medical devices designed to deliver high voltage electrical pulses to correct a fast or irregular heartbeat. Abbott has developed a firmware update to help mitigate the identified vulnerabilities.

CERT Australia recommends that healthcare providers initiate a discussion with affected patients, in relation to whether or not to apply the update, outlining the risks and benefits associated with applying the update. While not intended to serve as a substitute for clinician judgment as to whether the firmware update is advisable for a particular patient, CERT Australia recommends the following:

- Healthcare providers make patients aware of the "Online Patient Guide" and discuss the risk of performing the update, considering patient-specific issues [1].

Note that 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. Abbott has provided further details about this cybersecurity update on their website [2].

Healthcare providers and affected patients can access further information on Australian regulations and advice by contacting the Therapeutic Goods Administration [3].

DETAILS

Improper authentication

The device'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 ICD or CRT-D via RF communications.

Further information about this vulnerability may be available at CVE-2017-12712 [4].

Improper restriction of power consumption

The ICDs and CRT-Ds 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 device battery life.

Further information about this vulnerability may be available at CVE-2017-12714 [5].

REFERENCES

1. https://www.sjm.com/~/media/galaxy/hcp/resources-reimbursement/technical-resources/product-adviseries-archive/cyber-bpa-updates-icd-crtd/firmware-updates-icd-crtd-online-patient-guide-april2018.pdf?la=en
2. https://www.sjm.com/cyberupdate
3. https://www.tga.gov.au/
4. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12712
5. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12714

FEEDBACK

CERT Australia welcomes any feedback you may have with regard to this publication and/or the services we provide – info@cert.gov.au or 1300 172 499.

TRAFFIC LIGHT PROTOCOL

The following table lists the classification levels used in the traffic light protocol (TLP) and describes the restrictions on access and use for each classification level.

TLP classification	Restrictions on access and use
RED	**Access to and use by your CERT Australia security contact officer(s) only.** You must ensure that your CERT Australia security contact officer(s) does not disseminate or discuss the information with any other person, and you shall ensure that you have appropriate systems in place to ensure that the information cannot be accessed or used by any person other than your CERT Australia security contact officer(s).
AMBER	**Restricted internal access and use only.** Subject to the below, you shall only make AMBER publications available to your employees on a 'need to know basis' strictly for your internal processes only to assist in the protection of your ICT systems. In some instances you may be provided with AMBER publications which are marked to allow you to also disclose them to your contractors or agents on a 'need to know basis' – strictly for your internal purposes only to assist in the protection of your ICT systems.
GREEN	**Restricted to closed groups and subject to confidentiality.** You may share GREEN publications with external organisations, information exchanges, or individuals in the network security, information assurance or critical network infrastructure community that agree to maintain the confidentiality of the information in the publication. You may not publish or post on the web or otherwise release it in circumstances where confidentiality may not be maintained.
WHITE	**Not restricted.** WHITE publications are not confidential. They contain information that is for public, unrestricted dissemination, publication, web-posting or broadcast. You may publish the information, subject to copyright and any restrictions or rights noted in the information.
NOT CLASSIFIED	Any information received from CERT Australia that is not classified in accordance with the TLP must be treated as AMBER classified information, unless otherwise agreed in writing by the Attorney-General's Department.