HPRA
An tÚdarás Rialála Táirgí Sláinte
Health Products Regulatory Authority

Information Notice

Medical Devices

Potential Cybersecurity Vulnerabilities in Certain Medical Devices with Bluetooth Low Energy

HPRA Information Notice: IN2020(01) **Issue Date: 13th March 2020**

ISSUE

The HPRA are highlighting a cybersecurity vulnerability which affects medical devices worldwide. The vulnerability named SweynTooth impacts devices running on Bluetooth Low Energy (BLE) protocol. Many devices including medical devices such as pacemakers and insulin pumps are subject to this vulnerability.

These reported vulnerabilities may allow actors to crash devices, reboot devices and force them into a "deadlocked" state, or bypass security features. The exploit codes are available but we are not certain how widely circulated they are. It appears that these exploits may not be used directly from the internet, physical proximity (radio range) to the device being necessary.

The vulnerabilities were published by a group of researchers in Singapore on February 10th. See link below for further details:
https://asset-group.github.io/disclosures/sweyntooth/sweyntooth.pdf

The FDA released a Safety Communication on 3rd March 2020. This communication outlines the potential impact of the SweynTooth vulnerabilities and how they can be wirelessly exploited by an unauthorised user. It provides a list of system-on-a-chip manufacturers identified so far and recommended actions for manufacturers including mitigations and risk strategies, see link below for the full FDA Safety Communication:
https://www.fda.gov/medical-devices/safety-communications/sweyntooth-cybersecurity-vulnerabilities-may-affect-certain-medical-devices-fda-safety-communication

The HPRA will continue to assess new information concerning SweynTooth vulnerabilities and keep the public informed if significant new information becomes available. Following review of adverse incident data by various regulators there have been no known cases of this vulnerability being exploited although we are aware that it would be very difficult to identify.

We encourage manufacturers and users to report any incidents or concerns relating to this issue. These can be addressed to devicesafety@hpra.ie.

RECOMMENDATIONS

Recommendations for Manufacturers:

1 If your medical device or any device that communicates with your medical device uses BLE technology, evaluate if it is impacted by these vulnerabilities and develop risk mitigation plans.
2 Work with relevant stakeholders such as health care providers and patients to communicate mitigation measures and ensure that risks are managed.
3 Through your post market surveillance activities consider if the vulnerability has been exploited and investigate any signs of unusual behaviour.
4 Report any occurrences of exploitation of this vulnerability through your vigilance system.

Recommendations for Health Care Professionals

5 Where requested by device manufacturers, work with them to identify which medical devices in your facilities or in use by your patients could be affected by these vulnerabilities.
6 Ensure information issued by the manufacturer to mitigate the risks is acted upon and where appropriate, communicated to patients who use affected medical devices, including actions to take should they experience any unusual behaviour or have any concerns with their medical device.
7 Continue to remotely monitor devices as per normal procedure unless advised otherwise.

HPRA CONTACT INFORMATION

Health Products Regulatory Authority
Kevin O'Malley House
Earlsfort Centre
Earlsfort Terrace
Dublin 2

Telephone: +353-1-6764971
Fax: +353-1-6344033
E-mail: devicesafety@hpra.ie
Website: www.hpra.ie