|  |  |  |
| --- | --- | --- |
| ITU Logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | FG-AI4H-E-007 |
| **ITU-T Focus Group on AI for Health** |
| **Original: English** |
| **WG(s):** | Plen | Geneva, 30 May – 1 June 2019 |
| **DOCUMENT** |
| **Source:** | AHG-AI4HDS |
| **Title:** | Status report of the ad hoc group on AI for health device security and robustness benchmarking |
| **Purpose:** | Discussion |
| **Contact:** | Kai FuChina Telecommunications Technology Labs, China | Tel: +86 18310871563Email: fukai\_6@163.com  |
| **Contact:** | Ziyi YangCAICT, China | Tel: +86 18611172600Email: yangziyi@caict.ac.cn  |

|  |  |
| --- | --- |
| **Abstract:** | With the popularity of smart health devices, security issues such as data tampering and information leakage are becoming more and more serious. Currently, lacking mining and testing tools for vulnerability, which are directly applied to health device, making the situation worse. In order to deal with the situation, detecting and fixing the vulnerability in advance become more essential. Meanwhile, how to evaluate the robustness of emerging numerous AI-based health solutions is also an important work to investigate. This status report shows the recent work on health device vulnerability collecting and the plan for next steps. |

# Review of the background

Sharp increasing in health demand of aging population and worldwide medical resources shortage, provides a great market opportunity for the development of smart health equipment. The widespread use of smart health devices will generate a large amount of health data for more professional and effective analysis, further promoting the advancement of the health field. However, with the application of smart health equipment worldwide, its security issues have become increasingly prominent. At present, major organizations and enterprises pay close attention to applications and ignore security issues.

In addition, there are no effective means to discover and fix vulnerabilities, which may affect the widespread application of smart health devices. The development of AI, such as machine learning, provides the necessary conditions for solving the security problems of smart health devices. In this way, using AI to establish a set of vulnerability mining and testing tools can effectively solve the security problems of smart health device to promote its development worldwide.

# Update for collecting health device vulnerabilities

Roche Accu-Chek inform II instrument、Roche Accu-Chek Inform II Base Unit/Base Unit Hub and CoaguChek/cobas h232 Handheld Base Unit are hand-held blood test medical devices from Roche, Switzerland. They have vulnerabilities on permissions, access control, command execution, etc.



Several pacemaker products from Abbott Laboratories have vulnerabilities like unauthorized access, encryption error of sensitive data, product access limits, etc.



ZOOM LATITUDE PRMs is a portable heart rhythm management system for Boston Scientific that communicates with implantable pacemakers and defibrillators. It has vulnerabilities on hard-coded encryption, encryption error, etc.



MEDHOST Connex is a medical device of MEDHOST Corporation of the United States, which has vulnerabilities like hard-coded password bypass and sensitive information leakage. An attacker could use this vulnerability to obtain or modify sensitive and financial information of patients.



Drager Infinity Delta and others are medical monitor devices from Germany's Drager. There are security vulnerabilities in several Drager products. An attacker could use this vulnerability to obtain information such as the patient monitor address and wired network configuration.



Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump, which has a buffer overflow vulnerability, is a syringe infusion pump from Smiths Medical, UK. A remote attacker could exploit this vulnerability to execute arbitrary code on the target device.



NEMA DICOM is a set of medical digital image transmission protocol standards. An input validation error vulnerability exists in the DICOM Part 10 File Format from NEMA DICOM Standard 1995 to 2019b. The vulnerability come from a network system or product that does not properly validate the input data.



In addition, we collect the vulnerabilities including Fujifilm CR-IR 357 FCR Carbon X, a Fujifilm film imaging device from Fujifilm, GEInfinia/Infiniawith Hawkeye4, a medical imaging device from General Electric (GE), and a scanning camera for the medical industry in the US General Electric Company, as well as vulnerabilities of other devices like GE Healthcare Millennium MG, NC, and MyoSIGHT.

# Current vulnerability information collection source

* CVE: http://cve.mitre.org/index.html
* CNVD: http://www.cnvd.org.cn/
* CNNVD: http://www.cnnvd.org.cn/
* Anquanke: <https://www.anquanke.com/vul>

# Planned next steps

* Continue to collect information on health devices vulnerability
* Build a health device vulnerability library
* Based on the established vulnerability library, organize experts to discuss, analyse and summarize health device security assessment algorithms and benchmark principles
* Development of health device safety assessment and benchmark platform
* Validation of the platform
* Draft and issue a call for participation
* Cooperate with experts to investigate the methods for AI-based health solutions robustness evaluation
* Collect inputs from the regulatory group on relevant requirements for security and robustness

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_