Medical Device Advisory

Health Sciences Authority
Health Products Regulation Group
11 Biopolis Way #11-03 Helios
Singapore 138667
Website: www.hsa.gov.sg
Fax: 6478 9028

15 December 2023

CYBERSECURITY VULNERABILITIES (5GHOUL) POTENTIALLY AFFECTING MEDICAL DEVICES EMPLOYING 5G MODEMS

The Health Sciences Authority (HSA) would like to communicate regarding a recently discovered cybersecurity vulnerabilities called "**5Ghoul**". These vulnerabilities potentially affect commercial off-the-shelf (COTS) edge devices employing 5G modems. As of today, the **5Ghoul** vulnerabilities are known to affect 5G modems from 2 companies, *Qualcomm* and *MediaTek*.

Risk of Cybersecurity Vulnerabilities (5Ghoul)

2. The 5Ghoul vulnerabilities may be exploited to continuously launch attacks to drop the connection, freeze the connection that involve manual reboot or downgrade the 5G connectivity to 4G. This could potentially impact medical device systems which use the affected 5G modems and require network connection to function.

3. For more information regarding this issue, please refer to the following links. This includes information on how to identify if your medical devices could be affected by the vulnerabilities:

    - SingCERT alert (https://www.csa.gov.sg/alerts-advisories/alerts/2023/al-2023-161)
    - SUTD publication (https://www.5ghoul.com/)

Recommendations for Industry Stakeholders

4. To address these vulnerabilities, you are required to work with your manufacturers to carry out the following:

    i. Identify the medical devices affected by the vulnerabilities. Please refer to the above SingCERT Alert and SUTD publication;

    ii. Report to HSA at HSA_MD_INFO@hsa.gov.sg once you have identified affected medical devices;

    iii. Perform a risk assessment of the vulnerabilities and its impact in the context of your medical devices with reference to their intended use;

    iv. Develop risk mitigation plans, including interim work-around (e.g., segregation controls) to manage the risk until they can be patched;

    v. Ensure that the necessary security patches are rolled out to all affected devices locally in a timely manner; and

vi. Communicate with the healthcare institutions and the end users of your medical devices proactively and recommend necessary actions to reduce the risk and potential harm to the patients and users.

Recommendations for Healthcare Institutions and End-users

5. To manage these vulnerabilities, you are recommended to communicate with your medical device suppliers and manufacturers to find out if your device is affected by these vulnerabilities. Thereafter you should work with your suppliers to understand and implement the mitigation measures recommended by the medical device manufacturers.

6. In the meantime, HSA will continue to assess any new information on these vulnerabilities and will update our stakeholders on any significant safety information that arises. If you have any queries relating these vulnerabilities, you may contact us at HSA_MD_INFO@hsa.gov.sg.

Thank you.

Yours faithfully,

srama

DR SETHURAMAN RAMA
DIRECTOR (MEDICAL DEVICES)
MEDICAL DEVICES CLUSTER
HEALTH PRODUCTS REGULATION GROUP
HEALTH SCIENCES AUTHORITY