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

19 April 2021

CYBERSECURITY VULNERABILITIES (NAME:WRECK) AFFECTING FOUR TCP/IP NETWORK STACKS IN MEDICAL DEVICES

The Health Sciences Authority (HSA) would like to communicate regarding a recently discovered suite of cybersecurity vulnerabilities called “**NAME:WRECK**”. These vulnerabilities are related to Domain Name System (DNS) implementations and are found to affect the following four TCP/IP network stacks:

- FreeBSD version 12.1
- Nucleus NET version 4.3
- NetX version 6.0.1
- IPnet version VxWorks 6.6

Risk of Cybersecurity Vulnerabilities (NAME:WRECK)

2 If your medical devices are affected by any of these vulnerabilities, it will allow remote unauthorised access and allow malicious actors to conduct either Denial of Service (DoS) or Remote Code Execution (RCE), which will lead to failure of critical device functions. In order to address these vulnerabilities, security patches developed by the network stack developers, will have to be applied to the affected devices.

3 For more information, please refer to the following links for the detailed information regarding this issue, including the method to identify if your medical devices are affected by the vulnerabilities:

- SingCERT alert (https://www.csa.gov.sg/singcert/alerts/al-2021-024)
- Forescout publication (https://www.forescout.com/research-labs/namewreck/)

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 SingCERT Alert and Forescout publication above;

ii) Perform a risk assessment of the vulnerabilities and the impact in the context of your medical devices with reference to their intended use

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

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

v) 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.

5 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 BRANCH)
MEDICAL DEVICES CLUSTER
HEALTH PRODUCTS REGULATION GROUP
HEALTH SCIENCES AUTHORITY