

# Medical Device Advisory



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

22 December 2021

## **CYBERSECURITY VULNERABILITIES AFFECTING MEDICAL DEVICES UTILISING APACHE JAVA LOGGING LIBRARY LOG4J**

The Health Sciences Authority (HSA) would like to communicate regarding a recently discovered suite of cybersecurity vulnerabilities called the Apache Log4j Vulnerabilities. These vulnerabilities are affecting a variety of consumer and enterprise services, and applications, as well as medical devices that utilise Apache Java Logging Library Log4j.

### **Risk of Cybersecurity Vulnerabilities (Log4j)**

2. If your medical devices are affected by any of these vulnerabilities, it may allow an attacker to remotely gain full control of the affected system or conduct Denial of Service (DOS). In order to address these vulnerabilities, security patches 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/en/singcert/Advisories/ad-2021-010>)
  - Apache's Log4j vulnerabilities webpage (<https://logging.apache.org/log4j/2.x/security.html>)

### **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 Apache webpage above;
  - ii. Report to HSA at [HSA\\_MD\\_INFO@hsa.gov.sg](mailto:HSA_MD_INFO@hsa.gov.sg) once you have identified affected medical devices;
  - iii. Perform a risk assessment of the vulnerabilities and the 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](mailto: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