

Mindray Patient Monitor/Anesthesia
Cybersecurity Brief Log4j2

Intellectual Property Statement



are the trademarks, registered or otherwise, of Mindray in China and other countries. All other trademarks that appear in this document are used only for informational or editorial purposes. They are the property of their respective owners.

Manufacturer's Responsibility

Contents of this document are subject to change without prior notice.

All information contained in this document is believed to be correct. Mindray shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Background

On December 9, 2021 a high severity vulnerability (CVE-2021-44228) referred to as Log4j2 was published on GitHub which impacts Apache Log4J and the affected version ranges from 2.0 to 2.14.1. The exploitation of vulnerabilities can cause unauthenticated remote code execution.

Apache Log4J is open source Java code and that is widely used in middleware, development frameworks and web applications to record log information.

Mindray Course of Action

Mindray has not and does not use the identified Log4J in any product sold in North America, so there is no impact on Mindray products