How to mitigate the Spring CVE-2022-22965 vulnerability

The CVE-2022-22965 vulnerability

On March 30th, 2022, a 0-day exploit in the popular Java framework was discovered that results in Remote Code Execution (RCE) via data binding.

More about this vulnerability might be found at https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement.

What is affected

The VIVO core source is not a Spring framework-based application, but there is dependency on spring-beans and spring-context in [VIVO]/api/pom.xml.

Mitigation

- Please, check the version of spring-beans and spring-context in the [VIVO]/api/pom.xml file and check whether that version is listed as affected by this vulnerability at https://mvnrepository.com/artifact/org.springframework/spring-beans
    - If in the column Vulnerabilities (https://mvnrepository.com/artifact/org.springframework/spring-beans) there is a red link to one vulnerability, please do the following:
        - replace the version tag value (https://github.com/vivo-project/VIVO/blob/main/api/pom.xml#L46) with 5.3.18, as well as the version for spring-context with 5.3.18 (https://github.com/vivo-project/VIVO/blob/main/api/pom.xml#L51)
        - redeploy VIVO (mvn clean install)