Appendix - Software Composition Analysis Audit Template

This document contains a template that should be used to audit Software Composition Analysis report findings.

For mitigations that are implemented in the application software or are done through configuration, the developer must show where (filename and line number) the mitigations are implemented.

## Known Critical Vulnerabilities

|  |  |  |
| --- | --- | --- |
| **CVE-ID** | **Libraries And Frameworks** | **Developer Response** |
| [CVE-2022-22965](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965) | spring-beans-5.3.12.jar | The application is deployed as a Spring Boot executable jar therefore it is not vulnerable to the exploit. We also upgraded to spring-beans-5.3.18. |

## Known High Vulnerabilities

|  |  |  |
| --- | --- | --- |
| **CVE-ID** | **Libraries And Frameworks** | **Developer Response** |
| [CVE-2020-36518](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-36518) | jackson-databind-2.12.5.jar | Upgraded to safe jackson-databind version 2.13.2.2. |

## Known Medium Vulnerabilities

|  |  |  |
| --- | --- | --- |
| **CVE-ID** | **Libraries And Frameworks** | **Developer Response** |
| [CVE-2008-7271](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-7271) | javax.ws.rs-api-2.1.1.jar | This applies to Eclipse IDE which would only be for local development. Furthermore our team doesn’t use Eclipse IDE for local development. |
| [CVE-2010-4647](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4647) | javax.ws.rs-api-2.1.1.jar | This applies to Eclipse IDE which would only be for local development. Furthermore our team doesn’t use Eclipse IDE for local development. |
| [CVE-2021-22060](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060) | spring-beans-5.3.12.jar | Upgraded to safe spring-beans version 5.3.18. |
| [CVE-2022-22950](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950) | spring-beans-5.3.12.jar | Upgraded to safe spring-beans version 5.3.18. |

## Known Low Vulnerabilities

There were no issues reported for this section.

## Severity Unknown

There were no issues reported for this section.