# Casablanca OOF Security/Vulnerability Report

This table represents the known exploitable and non-exploitable vulnerabilities in third party packages used in the project.

There are no known vulnerabilities in the optf/osdf and optf/has repos

| Repository | Group | Impact Analysis | Action |
|---|---|---|---|
| optf/cmso | com.fasterxml.jackson.core:jackson-databind:2.9.7 | Confirmation of vulnerability. | Ensure that messages being de-serialized by Spring Boot are from trusted sources<br><br>☑ ~~OPTFRA-397~~ - CMSO Update to Spring Boot 2.1.3-RELEASE **CLOSED**<br><br>☑ ~~OPTFRA-390~~ - Add AAF AUthentication to CMSO **CLOSED** |
| | apache-httpclient:commons-httpclient | Confirmation of vulnerability. | Fixed & removed the jars<br><br>🔲 ~~OPTFRA-395~~ - CMSO - Fix security violations and increment version **CLOSED** |
| | org.codehaus.plexus | Confirmation of vulnerability | Fixed & removed the jars<br><br>🔲 ~~OPTFRA-395~~ - CMSO - Fix security violations and increment version **CLOSED** |
| | commons-collections | Confirmation of vulnerability | Fixed & removed the jars<br><br>🔲 ~~OPTFRA-395~~ - CMSO - Fix security violations and increment version **CLOSED** |
| | xerces:xercesImpl | Confirmation of vulnerability | Fixed & removed the jars<br><br>🔲 ~~OPTFRA-395~~ - CMSO - Fix security violations and increment version **CLOSED** |
| | commons-beanutils:commons-beanutils | Confirmation of vulnerability | Fixed & removed the jars<br><br>🔲 ~~OPTFRA-395~~ - CMSO - Fix security violations and increment version **CLOSED** |
| | dom4j:dom4j:1.6.1 | This dependency is pulled in by hibernate-core. dom4j is used internally in the hibernate library, which is not exposed to the external client.<br><br>The fix for CVE has been resolved in version 2.1.1 release which is included in spring-boot-data-jpa 2.1.0.RELEASE. | Request Exception.<br><br>To fix this would require upgrading spring-boot version to 2.1.0-RELEASE<br><br>☑ ~~OPTFRA-397~~ - CMSO Update to Spring Boot 2.1.3-RELEASE **CLOSED** |