Casablanca SO Security/Vulnerability Report

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

Repository	Group	Impact Analysis	Action
so/libs	com.fasterxml.jackson.core	False positive Jackson: can be an issue if we leave on default typing ○ In SO we do not use default typing. We use strict parsing and validation of deserialized data. ○ There is no unknown source data from which SO reads the application data (xml/json).	No Action. All of the existing jackson databind have vulnerabilities issues.
SO	org.eclipse.jetty	Pulled in by Springboot 1.5.13-RELEASE Note: We don't use jetty, but it is impractical to exclude	Planning for a spring boot upgrade to 2.0 in Dublin.
	com.fasterxml.jackson.core	False positive Jackson: can be an issue if we leave on default typing ○ In SO we do not use default typing. We use strict parsing and validation of deserialized data. ○ There is no unknown source data from which SO reads the application data (xml/json).	No Action All of the existing jackson databind have vulnerabilities issues.
	ch.qos.logback	False positive Pulled in by Springboot 1.5.13-RELEASE.	No Action in Casablanca. Planning for a spring boot upgrade to 2.0 in Dublin.
	org.slf4j	Pulled in by Springboot 1.5.13-RELEASE and also specified by SO There is no release version with non vulnerable available. application should not pass untrusted data into the constructor for the `EventData`class is vulnerable to this attack.	Planning for a spring boot upgrade to 2.0 in Dublin.
	org.apache.tomcat.embed	False positive Pulled in by Springboot 1.5.13-RELEASE Note: Tomcat CORS is turned off in our application Not really an issue since the feature is turned off.	No Action. Planning for a spring boot upgrade to 2.0 in Dublin.
	org.apache.commons	False positive SO doesn't use any email features in BPMN. Pulled in by Camunda 7.8.0	No Action for Casablanca. File for exception in Casablanca, Upgrade Camunda to 1.9.0 in Dublin
	org.slf4j-ext	False positive not used in SO code pulled from org.springframework.boot:spring-boot-starter-logging:jar:1.5.13.RELEASE	No Action in Casablanca.
	jetty-http	False positive no dependency found	Planning for a spring boot upgrade to 2.0 in Dublin.
	logback-classic	False positive no direct dependency. pulled from org.springframework.boot:spring-boot-starter-web:jar:1.5.13.RELEASE	Planning for a spring boot upgrade to 2.0 in Dublin.
	Jquery 1.10.2	False positive We dont have any UI code dependent on Jquery in SO. Pulled in by Springboot 1.5.13-RELEASE	Planning for a spring boot upgrade to 2.0 in Dublin.
	org.springframework.data	Used as the farmework of SO now, upgrade of the spring framework would resolve the issue. Pulled in by Springboot 1.5.13-RELEASE There is no non-vunerable release yet available. The `jQuery` package is vulnerable to Cross-Site Scripting (XSS) which is not used in SO currently.	Planning for a spring boot upgrade to 2.0 in Dublin.

	com. h2database	This is used for testing purpose only, no feature impact in production; no vulnerable free version yet The one currently used is with Highest Policy Threat:3	No Action for Casablanca
	commons-fileupload	False positive We dont use any of the file upload features directly in SO code Pulled in by Springboot 1.5.13-RELEASE	No Action required for Casablanca Planning for a spring boot upgrade to 2.0 in Dublin.
	org. googlecode. libphonenumber	False positive JavaScript library for parsing, formatting, and validating international phone numbers. We don't use libphonenumber in SO code, but it is impractical to exclude	No Action for Casablanca
	org. springframework	Artifact : Spring-web 5.0.9.RELEASE is pulled by the Springframework This is a required module, ugrade to springboot 2.0 would help in the resolution. This vulnerability affects applications that depend on either spring-webmvc or spring-webflux. Such applications must also have a registration for serving static resources (e.g. JS, CSS, images, and others), or have an annotated controller that returns an org.springframework.core.io.Resource. Currently SO is not found direct dependant on this. releases > 5.0.10.RELEASE would solve the issue,	No Action for Casablanca Planning for a spring boot upgrade to 2.0 in Dublin.
	javax. mail	False positive We aren't using any email features in SO. We don't use javax.mail, but it is impractical to exclude	No Action for Casablanca Planning for a spring boot upgrade to 2.0 in Dublin.
	org. springframework. security	No non-vunerable release available. Pulled by Springframework, cant be excluded. Switch User Processing Filter should not be configured to avoid this issue.	No Action for Casablanca Planning for a spring boot upgrade to 2.0 in Dublin.