Casablanca SDNC Security/Vulnerability Report

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

Note : the shaded lines in the table below are vulnerabilities inherited from upstream projects on which we depend. The direct dependency is listed in the Impact Analysis section. Many of these are from the OpenDaylight Oxygen distribution, on which much of SDNC is based. These vulnerabilities will be reported as CVEs to the OpenDaylight project so they can address them.

There are several vulnerabilities in used libraries that are noted. To mitigate the risk of exposure it is recommended that secure network design is used to avoid any unnecessary access to SDNC.

Repository	Group	Impact Analysis	Action
sdnc/apps, sdnc/oam	ch.qos.logback	**False positive** : only applies if logs are written to sockets (e.g. syslog), which does not apply in our case	No action needed
sdnc/oam	com.fasterxml	**False positive** : only applies if data format extension is used, which does not apply	No action needed
sdnc/oam	com.fasterxml	Inherited from OpenDaylight	Must be addressed in upstream OpenDaylight project
sdnc/apps, sdnc /northbound	com.fasterxml.jackson.core	Fixed in version 2.8.6	Will be updated to 2.8.9 in maintenance release (See ~~CCSDK-765~~ - Upgrade jackson version to 2.8.9 CLOSED)
sdnc/apps	com.fasterxml.jackson.core	Fixed in version 2.8.8.1	Will be updated to 2.8.9 in maintenance release (See ~~CCSDK-765~~ - Upgrade jackson version to 2.8.9 CLOSED)
sdnc/oam	com.fasterxml.jackson.core	Fixed in version 2.8.8.1	Will be updated to 2.8.9 in maintenance release (See ~~CCSDK-765~~ - Upgrade jackson version to 2.8.9 CLOSED)
sdnc/apps	com.fasterxml.jackson.core	Inherited from spring-boot	Must be addressed in upstream spring-boot
sdnc/apps	com.fasterxml.jackson.core	Inherited from spring-boot	Must be addressed in upstream spring-boot
sdnc/apps	com.fasterxml.jackson.core	Inherited from spring-boot	Must be addressed in upstream spring-boot
sdnc/apps	com.fasterxml.jackson.core	Inherited from spring-boot	Must be addressed in upstream spring-boot
sdnc/oam	com.google.guava	Inherited from gjsonpatch 0.2.1	Fix targeted for maintenance release (See ~~SDNC-536~~ - Upgrade zjsonpatch version to remediate vulnerabilities CLOSED)
sdnc/apps, sdnc /northbound	com.google.guava	Inherited from swagger-core	Must be addressed in upstream swagger-core
sdnc/oam	dom4j	Inherited from spring-boot	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc /northbound	javax.mail	Inherited from OpenDaylight	Must be addressed in upstream OpenDaylight project
sdnc/oam	org.apache.commons	Inherited from zjsonpatch 0.2.1	Fix targeted for maintenance release (See ~~SDNC-536~~ - Upgrade zjsonpatch version to remediate vulnerabilities CLOSED)

sdnc /northbound, sdnc/oam	org.apache. karaf.jaas	Inherited from OpenDaylight	Must be addressed in upstream OpenDaylight project
sdnc /northbound, sdnc/oam	org.apache. karaf.jaas	Inherited from OpenDaylight	Must be addressed in upstream OpenDaylight project
sdnc/oam	org.apache. logging. log4j	Inherited from spring-boot version 1.5.4-RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org.apache. tomcat. embed	Inherited from spring-boot version 1.5.4-RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org.apache. tomcat. embed	Inherited from spring-boot version 1.5.4-RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org.apache. tomcat. embed	Inherited from spring-boot version 1.5.4-RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org.apache. tomcat. embed	Inherited from spring-boot version 1.5.4-RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org.apache. tomcat. embed	Inherited from spring-boot version 1.5.4-RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org.apache. tomcat. embed	Inherited from spring-boot version 1.5.4-RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org.apache. tomcat. embed	Inherited from spring-boot version 1.5.4-RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org.apache. tomcat. embed	Inherited from spring-boot version 1.5.4-RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org. codehaus. jackson	Inherited from spring-boot	Must be addressed in upstream spring-boot
sdnc/oam	org. hibernate	Inherited from spring-boot version 1.5.4-RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org. springframe work	Fixed in version 4.3.15.RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/apps, sdnc /northbound	org. springframe work	Fixed in version 4.3.15.RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/apps	org. springframe work	Fixed in version 4.3.17.RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org. springframe work	Fixed in version 4.3.15.RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)

sdnc/apps, sdnc /northbound	org. springframe work	Fixed in version 4.3.17.RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/apps, sdnc /northbound	org. springframe work	Fixed in version 4.3.15.RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/apps, sdnc /northbound	org. springframe work	Fixed in version 4.3.17.RELEASE	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/apps	org. springframe work	Fixed in version 4.3.18	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/apps	org. springframe work	Fixed in version 4.3.18	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org. springframe work	Fixed in version 4.3.18	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org. springframe work	Fixed in version 4.3.18	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/apps, sdnc /northbound	org. springframe work	Fixed in version 4.3.18	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/apps, sdnc /northbound	org. springframe work	Fixed in version 4.3.18	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org. springframe work	Fixed in version 4.3.15	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org. springframe work	Fixed in version 4.3.18	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/apps	org. springframe work	Fixed in version 4.3.18	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org. springframe work.data	Fixed in version 1.13.11	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org. springframe work.data	Fixed in version 1.13.11	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/oam	org. springframe work.data	Fixed in version 1.13.12	Must upgrade to spring-boot version 2.1.0-RELEASE, which resolves this issue (~~SDNC-537~~ - Update to spring-boot 2.1.0-RELEASE CLOSED)
sdnc/apps	@stipsan /uikit	Not enough info in problem description to identify fixed version	Not enough info in problem description to identify fixed version
sdnc/oam	express	FALSE POSITIVE - only applies to older versions of node.js, < 0.9.4. We are using version 4.2.6	None needed
sdnc/oam	forwarded	FALSE POSITIVE - this code would not be executed in DG builder (it's included as part of base NodeRed platform, but not used)	None needed

sdnc/oam	fresh	FALSE POSITIVE - this code would not be executed in DG builder (it's included as part of base NodeRed platform, but not used)	None needed
sdnc/apps	handlebars	Inherited from swagger	Must be addressed in upstream swagger
sdnc/oam	jquery	FALSE POSITIVE - the vulnerable functionality is not used	None needed
sdnc/oam	jquery	FALSE POSITIVE - the vulnerable functionality is not used	None needed
sdnc/oam	jquery	FALSE POSITIVE - the vulnerable functionality is not used	None needed
sdnc/oam	serve-index	FALSE POSITIVE - the vulnerable functionality is not used	None needed