Casablanca DCAE 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
dcaegen2/analytics/tca-gen2	com.fasterxml.jackson.core	**False Positive** - we are not using the Jackson code in the manner that exposes the vulnerability. DCAEGEN2-765	Request exception
dcaegen2/analytics/tca	com.fasterxml.jackson.core	**False Positive** - we are not using the Jackson code in the manner that exposes the vulnerability. There is no use of `BeanDeserializerFactory` class in artifact "dcae-analytics-model". Hence we believe that this vulnerability report is a false positive.	No Action (same version as R2)
dcaegen2/analytics/tca	com.fasterxml.jackson.core	**False Positive** There is no use of either `UTF8StreamJsonParser` or `ReaderBasedJsonParser` class in artifact "dcae-analytics-model".	No Action (same version as R2)
dcaegen2/collectors/datafile	com.fasterxml.jackson.core	Only used by Swagger which get jackson in connection with API generation(from Spring). So if we exclude jackson, we will get runtime exception according to lack of jackson library. At the moment we haven't got any workaround. DCAEGEN2-764	Request exception
dcaegen2/collectors/hv-ves	com.fasterxml.jackson.core	**False Positive** Vulnerable artifacts are used only in following cases: 1. CSIT robot testsuites (hv-collector-dcae-app-simulator, hv-collector-xnf-simulator) which obviously does not pose a threat 2. Healthcheck mechanism which ignores client requests and uses (by dependency to hv-collector-utils) jackson to create response. Other modules affected are component-level-tests and coverage report which also are not used in production environment. DCAEGEN2-766	Request exception
dcaegen2/collectors/ves	com.fasterxml.jackson.core	**False Positive** The application is only vulnerable by using this component, when default typing is enabled and passing in untrusted data to be deserialization which is not the case here.	Request exception
dcaegen2/platform/inventory-api	com.fasterxml.jackson.core	**False Positive** According to these description, and the fact that the org.onap.dcaegen2.platform:inventory-api code does not enable use of global type information, using Class name as the type id, we believe that this report is a false positive. DCAEGEN2-768	Request exception
dcaegen2/services/mapper	com.fasterxml.jackson.core	**False Positive** There is no use of `BeanDeserializerFactory` class in snmpmapper. Hence we believe that this vulnerability report is a false positive. DCAEGEN2-769	Request exception
dcaegen2/services/prh	com.fasterxml.jackson.core	Only used by Swagger which get jackson in connection with API generation(from Spring). So if we exclude jackson, we will get runtime exception according to lack of jackson library. DCAEGEN2-770	Request exception

dcaegen2/collectors/ves	org.apache.tomcat.embed	Requires moving to tomcat-embed-websocket:8.5.34	Added 10/29 - Request exception ☑ ~~**DCAEGEN2-927**~~ - Address VESCollector vulnerability reported R3 RC1 phase CLOSED
dcaegen2/platform/inventory-api	org.postgresql	Requires moving postgresql to 42.2.5	Added 10/29 - Request exception ☑ ~~**DCAEGEN2-926**~~ - Address InventoryAPI vulnerabilities reported - R3 RC1 phase CLOSED
dcaegen2/analytics/tca-gen2	io.undertow	No non-vulnerable version available.	Request exception
dcaegen2/analytics/tca	com.google.guava	No non-vulnerable version available.	Request exception
dcaegen2/analytics/tca	commons-codec	Not applicable as base32 encoding is not used	Request exception
dcaegen2/collectors/datafile	org.springframework	Newer non vulnerable version available (5.1.0.RELEASE)	Upgrade to newer version ☑ ~~**DCAEGEN2-869**~~ - Address critical vulnerability for DFC CLOSED
dcaegen2/collectors/datafile	com.jcraft	Not applicable; as the application doesn't run on windows	Request exception
dcaegen2/collectors/hv-ves	org.apache.kafka	Newer non vulnerable version available	Request exception
dcaegen2/collectors/ves	org.springframework	Requires moving to spring-web:5.1.1.RELEASE	Added 10/29 - Request exception ☑ ~~**DCAEGEN2-927**~~ - Address VESCollector vulnerability reported R3 RC1 phase CLOSED
dcaegen2/collectors/ves	com.googlecode.libphonenumber	Not applicable.	Request exception
dcaegen2/collectors/ves	javax.mail	Not applicable; as the specified method is not invoked	Request exception
dcaegen2/collectors/ves	org.springframework.security	spring-security-web:5.0.6.RELEASE flagged No non-vulnerable version available.	Added 10/30 - Request exception
dcaegen2/platform/inventory-api	org.postgresql : postgresql	No non-vulnerable version available.	Request exception
dcaegen2/services/mapper	dom4j : dom4j :	Not applicable; as the specified method is not invoked	Request exception
dcaegen2/services/mapper	org.springframework : spring-web	No non-vulnerable version available & Unknown license reported	Request exception
dcaegen2/services/mapper	ognl : ognl : 3.0.9	Newer non vulnerable version available	Upgrade to newer version available ☑ ~~**DCAEGEN2-871**~~ - Address critical vulnerability for Mapper CLOSED
dcaegen2/services/mapper	org.postgresql : postgresql : 42.2.4	No non-vulnerable version available.	Request exception
dcaegen2/services/mapper	xerces : xercesImpl : 2.12.0	No non-vulnerable version available.	Request exception

dcaegen2 /services/prh	org. springframework : spring-web	Newer non vulnerable version available	Upgrade to newer version available ~~DCAEGEN2-870~~ - Address critical vulnerability for PRH CLOSED