

DCAE R10 Vulnerability - SECCOM Report

NOTE: This page is copy of Jakarta DCAE report created by SECCOM (excluded CVE info); any update should be done on parent page.

The tables contain the recommended package version upgrades for outdated direct dependencies with Critical or Severe vulnerabilities identified by NexusIQ. These packages must be upgraded by M2/M3 or a request for a waiver must be requested from SECCOM and the TSC.

- **Priority 1** recommendations have at least one Critical vulnerability.
- **Priority 2** recommendations contain at least one Severe vulnerability, and no Critical vulnerabilities.
- There are four status values:
 - **OPEN** - required upgrade identified
 - **IN PROGRESS** - project working on the upgrade
 - **COMPLETE** - package has been upgraded to the recommended version
 - **WAIVER** - project granted a waiver for the upgrade because of technical or resource constraints

When the upgrade of the package is complete change the status in the table to **COMPLETE**.

If a waiver is granted, change the status to **WAIVER**.

When the status of all direct dependency replacements is **COMPLETE** or **WAIVER**, the Jira ticket should be closed.

dcaegen2-analytics-tca-gen2

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
OPEN	2	io.springfox : springfox-swagger2 : 3.0.0	5	???	Already on latest; no non-vulnerable version available
OPEN	2	undertow-core : 2.2.7.Final	5	2.2.14	2.2.14.Final
			5		

dcaegen2-collectors-datafile

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
OPEN	1	spring-web : 5.3.6	9	5.3.13	5.3.13 or 5.3.14
			7		
			4		
OPEN	2	io.springfox : springfox-swagger2 : 3.0.0	5	???	Already on latest; no non-vulnerable version available

onap-dcaegen2-collectors-restconf

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
OPEN	1	ch.qos.logback : logback-core : 1.3.0-alpha0	8	1.2.10	1.2.10
OPEN	1	com.google.code.gson : gson : 2.8.5	7	2.8.9	2.8.9
OPEN	2	io.springfox : springfox-swagger2 : 3.0.0	5	???	Already on latest; no non-vulnerable version available
	1	com.fasterxml.jackson.core : jackson-databind : 2.11.0	10	2.12.6	2.12.6

dcaegen2-collectors-hv-ves

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
OPEN	1	com.google.code.gson : gson : 2.8.6	7	2.8.9	2.8.9

dcaegen2-collectors-ves

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
OPEN	1	com.google.code.gson : gson : 2.8.6	7	2.8.9	2.8.9
OPEN	2	io.netty : netty-codec-http : 4.1.59.Final	5	4.1.70.Final	4.1.73.Final
OPEN	2	io.springfox : springfox-swagger2 : 3.0.0	5	???	Already on latest; no non-vulnerable version available
		org.apache.logging.log4j : log4j-core : 2.16.0			2.17.1

dcaegen2-platform-mod-genprocessor

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
	1	com.fasterxml.jackson.core : jackson-databind : 2.11.0	10	2.12.6	2.12.6
OPEN	2	nifi-utils : 1.9.2	5		retain current version due to dependency with upstream nifi version on designer module

dcaegen2-platform-mod2-auth

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
OPEN	1	com.google.code.gson : gson : 2.8.6	7	2.8.9	POC components; not part of ONAP deployment
OPEN	1	com.squareup.okhttp3 : okhttp : 4.0.1	7	4.9.3	POC components; not part of ONAP deployment

dcaegen2-platform-mod2-catalog

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
OPEN	1	com.google.code.gson : gson : 2.8.6	7	2.8.9	POC components; not part of ONAP deployment
OPEN	1	com.squareup.okhttp3 : okhttp : 4.0.1	7	4.9.3	POC components; not part of ONAP deployment
OPEN	1	io.springfox : springfox-swagger-ui : 2.9.2	9 6 6	3.0.0	POC components; not part of ONAP deployment
OPEN	2	io.springfox : springfox-swagger2 : 2.9.2	5	3.0.0	POC components; not part of ONAP deployment

dcaegen2-platform-mod-runtimeapi

Status	Priority	Component name and version	CVE	Threat level	Recommended version	Project's assessment (Target for J)

caegen2-services-kpi-computation-ms

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
--------	----------	----------------------------	--------------	---------------------	-------------------------------------

OPEN	1	ch.qos.logback : logback-core : 1.3.0-alpha0	8	1.2.10	1.2.10
OPEN	1	org.springframework : spring-web : 5.3.7	9 4	5.3.13	5.3.14
	1	com.fasterxml.jackson.core : jackson-databind : 2.11.0	10	2.12.6	2.12.6
OPEN	2	io.undertow : undertow-core : 2.2.8.Final	5 5	2.2.14.Final	2.2.14.Final
		org.springframework : spring-webmvc : 5.3.7	6		5.3.14

dcaegen2-services-bbs-event-processor

Status	Priority	Component name and version	CVE	Threat level	Recommended version	Project's assessment

dcaegen2-services-mapper

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
	1	com.fasterxml.jackson.core : jackson-databind : 2.11.2	10	2.12.6	2.12.6
		org.apache.logging.log4j: log4j-core:2.16.0			2.17.1
OPEN	1	com.google.code.gson : gson : 2.8.5	7	2.8.9	2.8.9
OPEN	1	xstream : 1.4.16	8	1.4.18	1.4.18
OPEN	2	xercesImpl : 2.12.1	5	???	Already on latest; no non-vulnerable version available

dcaegen2-services-pm-mapper

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
OPEN	1	com.google.code.gson : gson : 2.8.5	7	2.8.9	2.8.9
OPEN	2	undertow-core : 2.2.9.Final	5 4 4	2.2.14.Final	2.2.14.Final 2.2.16.Final

dcaegen2-services-prh

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
OPEN	1	org.apache.tomcat.embed : tomcat-embed-websocket : 9.0.48	7	10.1.0M7	Either 10.1.0-M8 or 9.0.56
OPEN	1	org.springframework : spring-web : 5.3.8	9 4	5.3.13 RELEASE	5.3.14

dcaegen2-services-sdk

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment
OPEN	1	ch.qos.logback : logback-core : 1.3.0-alpha0	8	1.2.10	1.2.10
OPEN	1	com.google.code.gson : gson : 2.8.5	7	2.8.9	2.8.9

		org.springframework : spring-webflux : 5.3.1	6		5.3.14
--	--	--	---	--	--------

dcaegen2-services-son-handler

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment
	1	com.fasterxml.jackson.core : jackson-databind : 2.11.0	10	2.12.6	2.12.6
OPEN	1	ch.qos.logback : logback-core : 1.3.0-alpha0	8	1.2.10	1.2.10
OPEN	1	org.springframework : spring-web : 5.3.7.RELEASE	9	5.3.13 RELEASE	5.3.14
			4		
		org.springframework : spring-webmvc : 5.3.7	6		5.3.14
OPEN	1	org.apache.tomcat.embed : tomcat-embed-core : 9.0.46	6	10.1.0-M7	9.0.50 or 10.1.0-M8

dcaegen2-services-slice-analysis-ms

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment
	1	com.fasterxml.jackson.core : jackson-databind : 2.11.0	10	2.12.6	2.12.6
OPEN	1	ch.qos.logback : logback-core : 1.3.0-alpha0	8	1.2.10	1.2.10
OPEN	1	org.springframework : spring-web : 5.3.7.RELEASE	9	5.3.13 RELEASE	5.3.14
			4		
		org.springframework : spring-webmvc : 5.3.7	6		5.3.14
OPEN	2	org.apache.tomcat.embed : tomcat-embed-core : 9.0.46	6	10.1.0-M7	9.0.50 or 10.1.0-M8

dcaegen2-platform-mod2-helmgenerator

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
		com.fasterxml.jackson.core : jackson-databind : 2.10.3	10		2.12.6
		com.squareup.okhttp3 : okhttp : 4.0.1	5		4.9.3
		commons-io : commons-io : 2.4			2.11.0

dcaegen2-platform-ves-openapi-manager

Status	Priority	Component name and version	Threat level	Recommended version	Project's assessment (Target for J)
		com.fasterxml.jackson.core : jackson-databind : 2.9.4	10		2.12.6