Jakarta CPS

The tables contain the recommended package version upgrades for outdated direct dependencies with Critical or Severe vulnerabilities identified by NexusIQ.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 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.

cps-cps-tbdmt

Status	Priority	Component name and version	CVE	Threat level	Recommended version	Project's assessment
OPEN	1	com.google.code.gson : gson : 2.8.6	SONATYPE-2021-1694	10	2.8.9	
OPEN	1	org.springframework : spring-web : 5.3.7	CVE-2016-1000027 CVE-2021-22096	10	5.3.13	
OPEN	2	org.eclipse.jetty : jetty-http : 9.4.40.v20210413	CVE-2021-34429	6	11.0.7	
OPEN	2	org.eclipse.jetty : jetty-servlets : 9.4.40.v20210413	CVE-2021-28169	6	11.0.7	

cps-cps-temporal

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

cps

Status	Priority	Component name and version	CVE	Threat level	Recommended version	Project's assessment
OPEN	1	com.google.code.gson : gson : 2.8.8	SONATYPE-2021-1694	10	2.8.9	
OPEN	1	org.springframework : spring-web : 5.3.10	CVE-2016-1000027 CVE-2021-22096	10	5.3.13	

cps-ncmp-dmi-plugin

Status	Priority	Component name and version	CVE	Threat level	Recommended version	Project's assessment
OPEN	1	com.google.code.gson : gson : 2.8.8	SONATYPE-2021-1694	10	2.8.9	