

JoramMQ 1.18

Code security & quality

Ce rapport se base sur les exécutions des plugins Maven de SonarQube et du plugin OWasp sur les bases de code de Joram et JoramMQ.

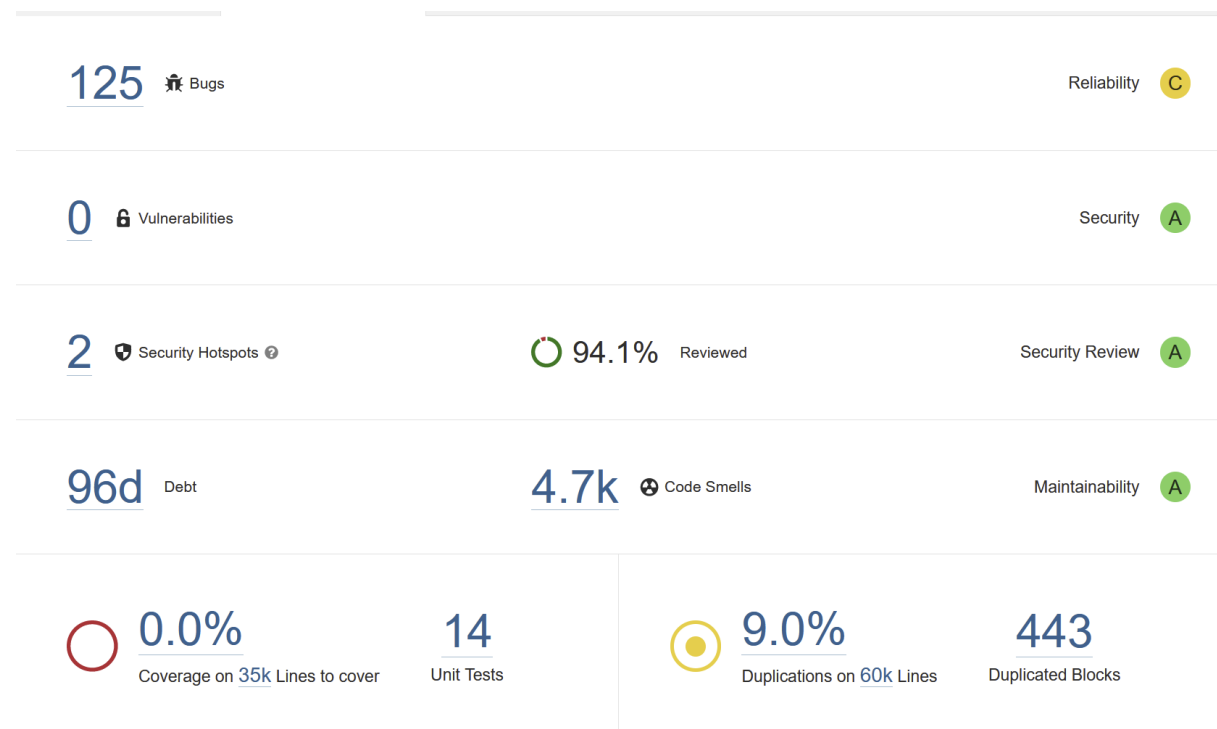
JoramMQ 1.18

SonarQube

JoramMQ est régulièrement analysé par des exécutions explicites du plugin Maven de SonarQube. La version utilisée est la version 9.7.1 de SonarQube.

Ce rapport se base sur l'exécution du 25/09/2023 et correspond à la version 1.18.0 de JoramMQ.

Overview



Bugs

- 0 'Blocker', 0 'Critical'
- 74 'Major'
 - 53 Interrupted exceptions non propagées.

- 20 usages de notify (SQ encourage l'usage de notifyAll ce qui ne correspond pas au besoin).
- 51 'Minor'
 - 23 valeurs de retour ignorées.

Vulnerabilities

- 0

Security Hotspots

- 2 'Low' : usage de fichiers temporaires.

OWASP

Le plugin OWASP version: 8.4.0 est utilisé pour faire des scans réguliers des dépendances de JoramMQ, ces dépendances sont systématiquement scannées avant la sortie de chaque nouvelle version.

L'unique vulnérabilité signalée dans la version 1.17.0 du broker JoramMQ est :

- guava-21.0.jar
 - Usage : Module de persistance TxLog utilisant la version Java de LevelDB.
 - bundle/txlog.java
 - Vulnerability IDs
 - cpe:2.3:a:google:guava:21.0:*:*:*:*:*
 - pkg:maven/com.google.guava:guava@21.0
 - HIGH 3

D'autres vulnérabilités sont présentes dans des composants optionnels de JoramMQ :

- amqp-client-2.2.0.jar
 - Usage : Uniquement en cas d'utilisation explicite du bridge AMQP.
 - bundle/joram-mom-extensions-amqp.jar
 - pkg:maven/com.rabbitmq/amqp-client@2.2.0
 - MEDIUM 1
- derby.jar
 - Usage : Uniquement en cas d'utilisation explicite de la base de données Derby.
 - Vulnerability IDs
 - cpe:2.3:a:apache:derby:10.11.1000002.1629631:*:*:*:*:*
 - MEDIUM 1
- joram-mom-extensions-ftp-5.21.0-SNAPSHOT.jar
 - Usage : Uniquement en cas d'utilisation explicite du bridge FTP.
 - bundle/joram-mom-extensions-ftp.jar
 - Vulnerability IDs
 - cpe:2.3:a:ftp_project:ftp:5.21.0:snapshot:*:*:*:*:*
 - Repose sur la seule présence du terme FTP dans le nom du package.
 - HIGH 1
- log4j-1.2.12.java

- Usage : Uniquement en cas d'utilisation explicite du connecteur Stomp.
 - bundle/joram-tools-jasp.jar
- Vulnerability IDs
 - cpe:2.3:a:apache:log4j:1.2.12:*:*:*:*:*
- CRITICAL 7
- netty-3.10.6.Final.jar
 - Usage : Uniquement en cas d'utilisation d'une configuration distribuée avec BatchNetwork.
 - bundle/batchnetwork.jar
 - Vulnerability IDs
 - cpe:2.3:a:netty:netty:3.10.6:*:*:*:*:*
 - pkg:maven/io.netty/netty@3.10.6.Final
 - CRITICAL 13

Des vulnérabilités sont aussi présentes dans 2 logiciels additionnels de JoramMQ :

- Simulateur MQTT : nécessite un usage explicite par le client.
 - graal-sdk-21.1.0.jar
 - LOW 1
 - javax.json-1.0.4.jar
 - Vulnerability IDs
 - cpe:2.3:a:json-java_project:json-java:1.0.4:*****
 - HIGH 1
 - json-20140107.jar
 - Vulnerability IDs
 - cpe:2.3:a:json-java_project:json-java:*****
 - HIGH 1
 - oshi-json-3.4.3.jar
 - Vulnerability IDs
 - cpe:2.3:a:json-java_project:json-java:3.4.3:*****
 - HIGH 1
- Console HawtIO : nécessite un usage explicite par le client. Ces vulnérabilités sont présentes dans le fichier jorammq-hawtio.war de la livraison.
 - jorammq-hawtio-1.5.11.war
 - Vulnerability IDs
 - cpe:2.3:a:hawt:hawtio:1.5.11:*****
 - cpe:2.3:a:hawt.io:hawtio:1.5.11:*****
 - pkg:maven/io.hawt/jorammq-hawtio@1.5.11
 - CRITICAL 1
 - jorammq-hawtio-1.5.11.war: log4j-1.2.17.jar
 - Vulnerability IDs
 - cpe:2.3:a:apache:log4j:1.2.17:*****
 - pkg:maven/log4j/log4j@1.2.17
 - CRITICAL 6
 - jorammq-hawtio-1.5.11.war: infinispn-core-5.3.0.Final.jar
 - Vulnerability IDs
 - cpe:2.3:a:infinispn:infinispn:5.3.0:*****
 - pkg:maven/org.infinispn/infinispn-core@5.3.0.Final
 - CRITICAL 6

- jorammq-hawtio-1.5.11.war: hawtio-plugin-mbean-1.5.11.jar
 - Vulnerability IDs
 - cpe:2.3:a:hawt:hawtio:1.5.11:****:*
 - cpe:2.3:a:hawt.io:hawtio:1.5.11:****:*
 - pkg:maven/io.hawt/hawtio-plugin-mbean@1.5.11
 - CRITICAL 1
- jorammq-hawtio-1.5.11.war: example-infinispan-1.5.11.jar
 - Vulnerability IDs
 - cpe:2.3:a:infinispan:infinispan:1.5.11:****:*
 - pkg:maven/io.hawt.example.services/example-infinispan@1.5.11
 - CRITICAL 6
- jorammq-hawtio-1.5.11.war: example-dozer-models-1.5.11.jar
 - Vulnerability IDs
 - cpe:2.3:a:dozer_project:dozer:1.5.11:****:*
 - pkg:maven/io.hawt.example.services/example-dozer-models@1.5.11
 - CRITICAL 1
- jorammq-hawtio-1.5.11.war: jolokia-core-1.5.0.jar
 - Vulnerability IDs
 - cpe:2.3:a:jolokia:jolokia:1.5.0:****:*
 - pkg:maven/org.jolokia/jolokia-core@1.5.0
 - HIGH 1
- jorammq-hawtio-1.5.11.war: jackson-mapper-asl-1.9.2.jar
 - Vulnerability IDs
 - cpe:2.3:a:fasterxml:jackson-mapper-asl:1.9.2:****:*
 - HIGH 1
- jorammq-hawtio-1.5.11.war: commons-lang3-3.1.jar
 - Vulnerability IDs
 - cpe:2.3:a:apache:commons_net:3.1:****:*
 - pkg:maven/org.apache.commons/commons-lang3@3.1
 - MEDIUM 1

Joram 5.21.0

Joram est un composant clé de JoramMQ, la version embarquée dans JoramMQ 1.17 est Joram 5.21.

SonarQube

Joram est automatiquement analysé chaque dimanche sur la plateforme OW2, la version utilisée est la dernière version LTS de SonarQube (Version 9.9.1).

Ce rapport se base sur l'exécution du 25/09/2023 et correspond à la version 5.21.0 de Joram :

- <https://sonarqube.ow2.org/dashboard?id=org.ow2.joram%3Aparent>

Overview


[249](#) 🐛 Bugs

Reliability C

[757](#) 🔒 Vulnerabilities

Security B

[14](#) 🛡️ Security Hotspots ⓘ


 82.5% Reviewed

Security Review A


[219d](#) Debt

[11k](#) 🕒 Code Smells

Maintainability A

 [1.2%](#)
Coverage on [78k](#) Lines to cover

[9](#)
Unit Tests

 [33.2%](#)
Duplications on [129k](#) Lines

[1.1k](#)
Duplicated Blocks

Bugs

- 0 'Blocker', 0 'Critical'
- 186 'Major'
 - 131 InterruptedException non propagées.
 - 42 usages de notify (SQ encourage l'usage de notifyAll ce qui ne correspond pas au besoin).
- 63 'Minor'

Vulnerabilities

- 0 'Blocker', 0 'Critical', 0 'Major'
- 764 'Minor'
 - 503 attributs 'public' dans une classe.
 - 197 attributs 'public static' non final.
 - 33 valeurs de retour ignorées.
 - 24 attributs mutables publics.

Security Hotspots

- 14 'Low' : 2 usages de fichiers temporaires, et 12 expansions de fichiers compressés (rar).

OWASP

Le plugin OWASP 8.4.0 est utilisé pour faire des scans réguliers des dépendances de Joram, ces dépendances sont systématiquement scannées avant la sortie de chaque nouvelle version.

Les vulnérabilités signalées dans la version 5.21.0 du broker Joram sont strictement identiques à la version antérieure (5.20.0) :

- log4j-1.2.12.jar
 - Usage : Connecteur STOMP déprécié, jar log4j non livré.
 - bundle/joram-tools-jasp.jar
 - Vulnerability IDs
 - cpe:2.3:a:apache:log4j:1.2.12:*.***:***.*
 - pkg:maven/log4j/log4j@1.2.12
 - CRITICAL 6 Highest 15
- amqp-client-2.2.0.jar
 - Usage : bridge AMQP
 - bundle/joram-mom-extensions-amqp.jar
 - pkg:maven/com.rabbitmq/amqp-client@2.2.0
 - MEDIUM 1 43