COMMUNITY mojaloop MEETING

Code Quality & Security Workstream Update

Quarterly Open-Source Software(OSS) Scan Report – 26 July 2022

Presenter

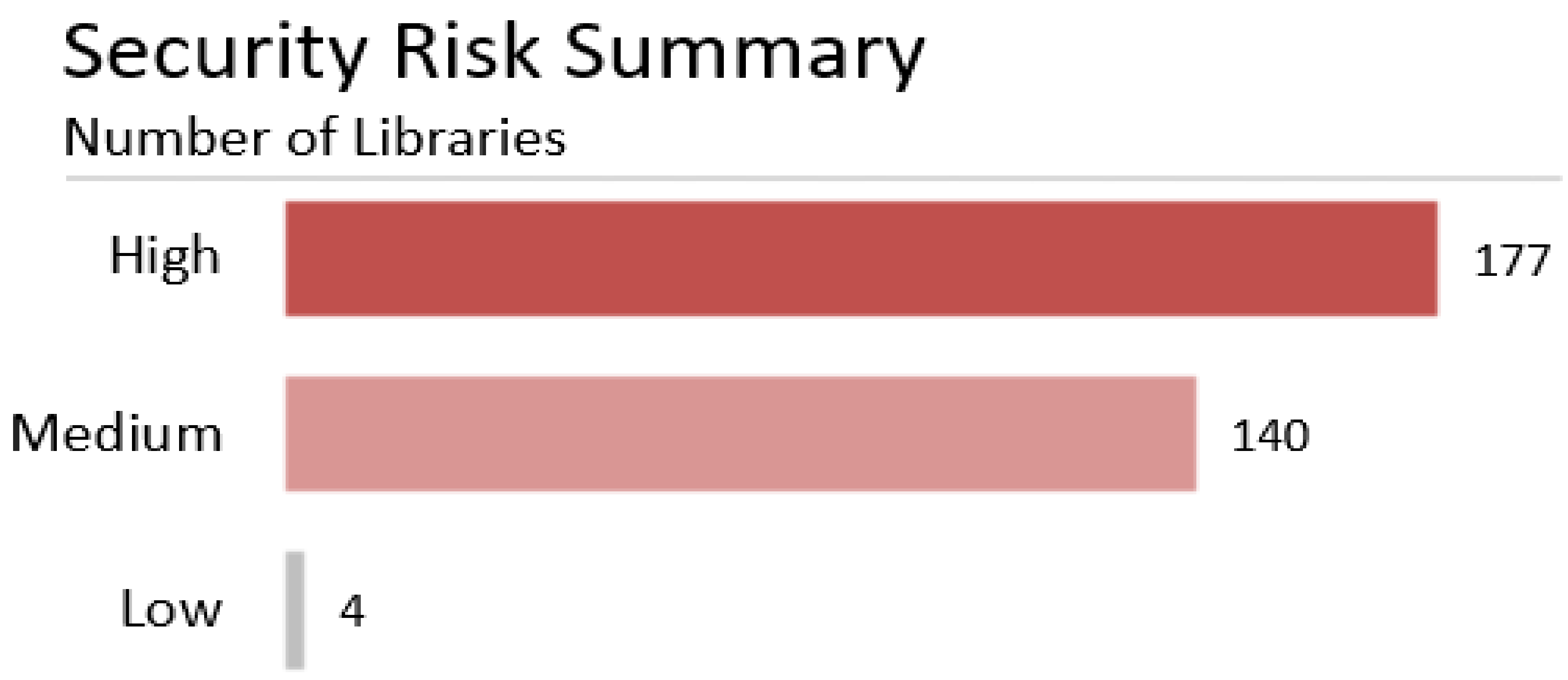
Godfrey Kutumela

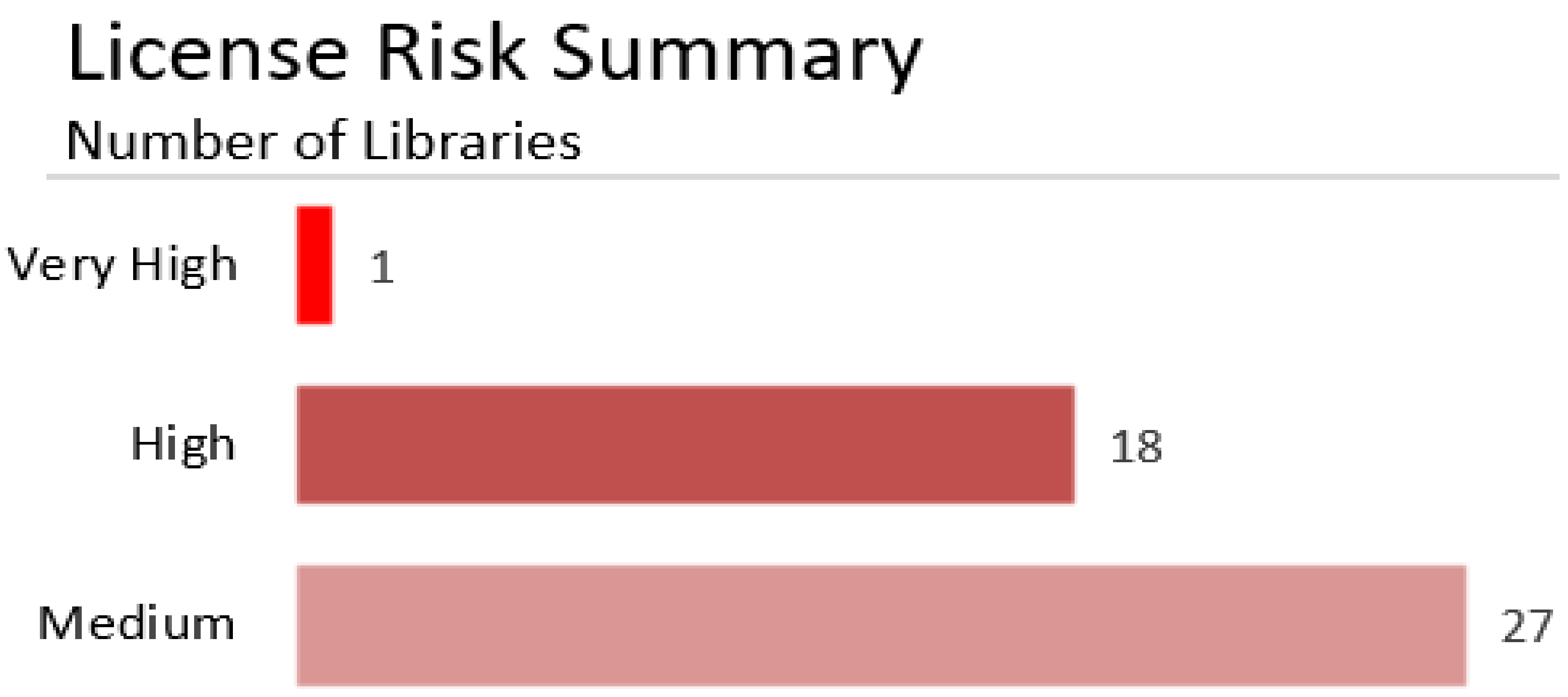
PI Objectives

Perform a quarterly open-source software (OSS) scan to detect and mitigate software supply chain risks

- Open-Source License Assessment: To ensure compliance with Mojaloop open-source license policy – Apache 2.0 license.
- Open-Source Security Assessment: To ensure that libraries used are not vulnerable and outdated to minimize security risks.

Findings Summary



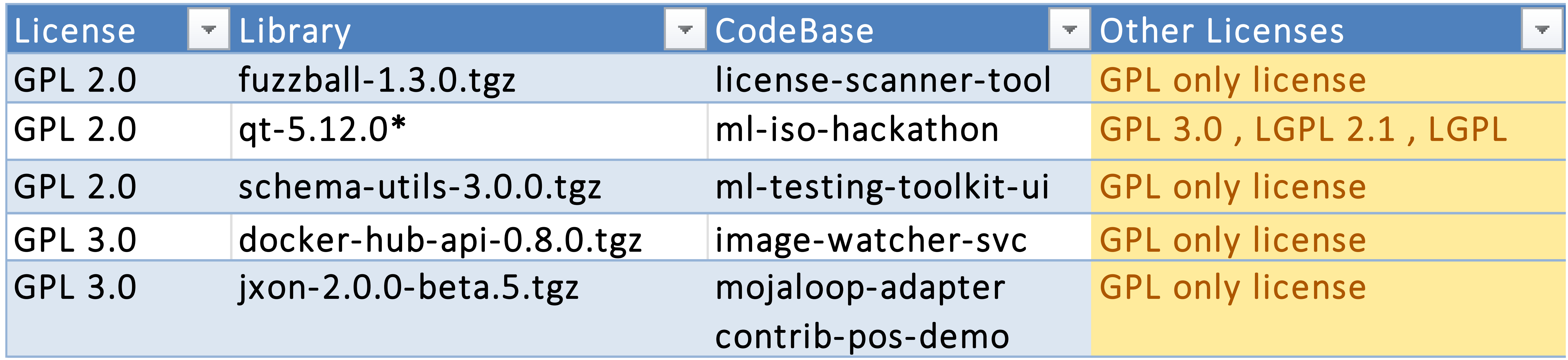


Security Risk Analysis

- **All high security findings affects only transitive dependencies** and requires a review of the dependency strategy to ensure that we can mitigate as much as feasible.
- **5 libraries** (convict-6.0.0.tgz, ejs-2.7.4.tgz, handlebars-4.7.6.tgz, json-pointer-0.6.1.tgz, url-parse-1.5.3.tgz have many vulnerabilities classified as critical according to CVSS3 scoring (>9) and should be first prioritized for remediation.

License Risk Analysis

- ○ **14 libraries** have alternative permissive licenses (Apache, BSD, MIT), reducing the risk to low.
- ○ **5 libraries** have GPL license only which makes them non-compliant with the Mojaloop Apache 2.0 license policy



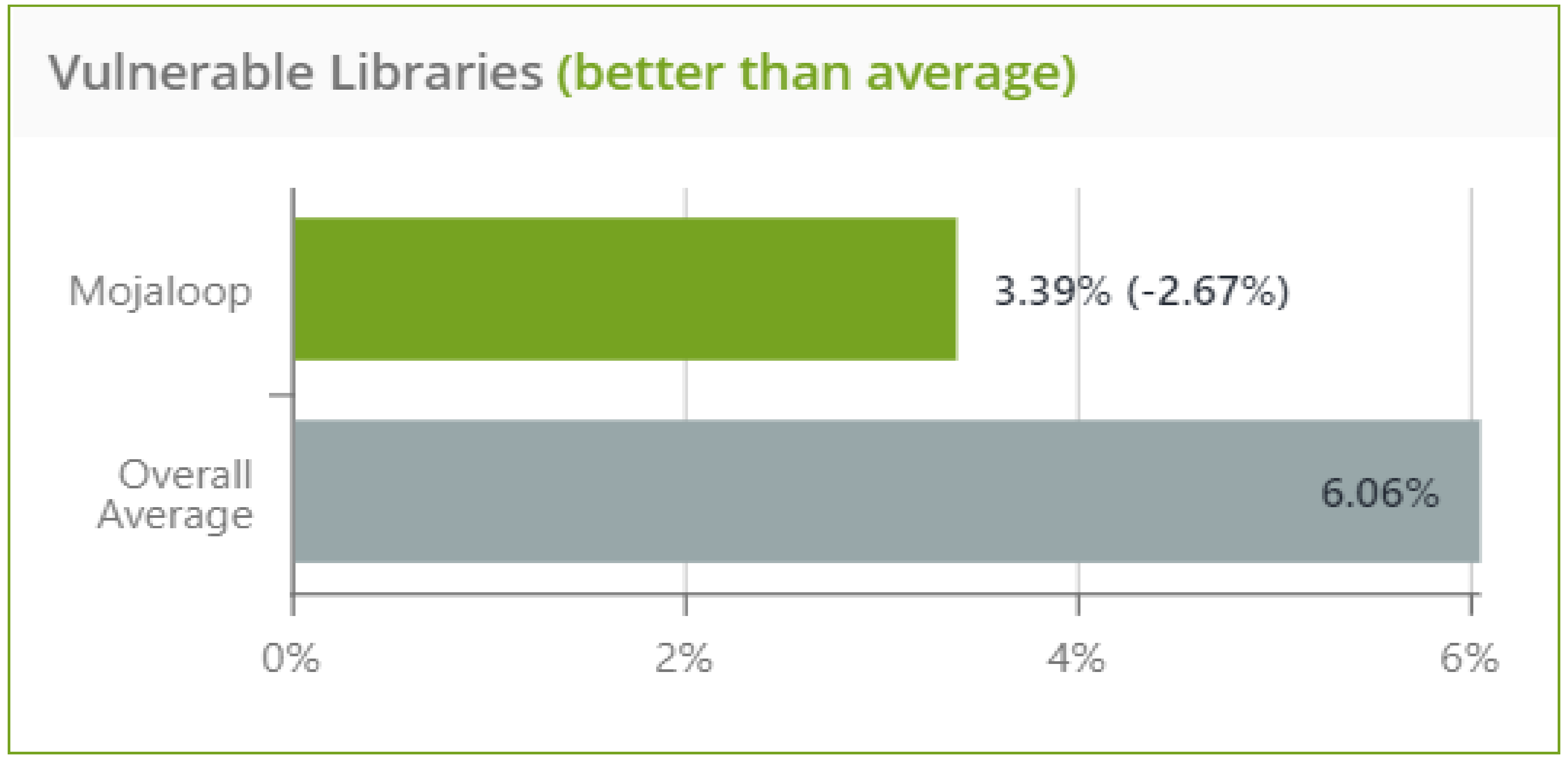
License	Library	CodeBase	Other Licenses
GPL 2.0	fuzzball-1.3.0.tgz	license-scanner-tool	GPL only license
GPL 2.0	qt-5.12.0*	ml-iso-hackathon	GPL 3.0 , LGPL 2.1 , LGPL
GPL 2.0	schema-utils-3.0.0.tgz	ml-testing-toolkit-ui	GPL only license
GPL 3.0	docker-hub-api-0.8.0.tgz	image-watcher-svc	GPL only license
GPL 3.0	jxon-2.0.0-beta.5.tgz	mojaloop-adapter contrib-pos-demo	GPL only license

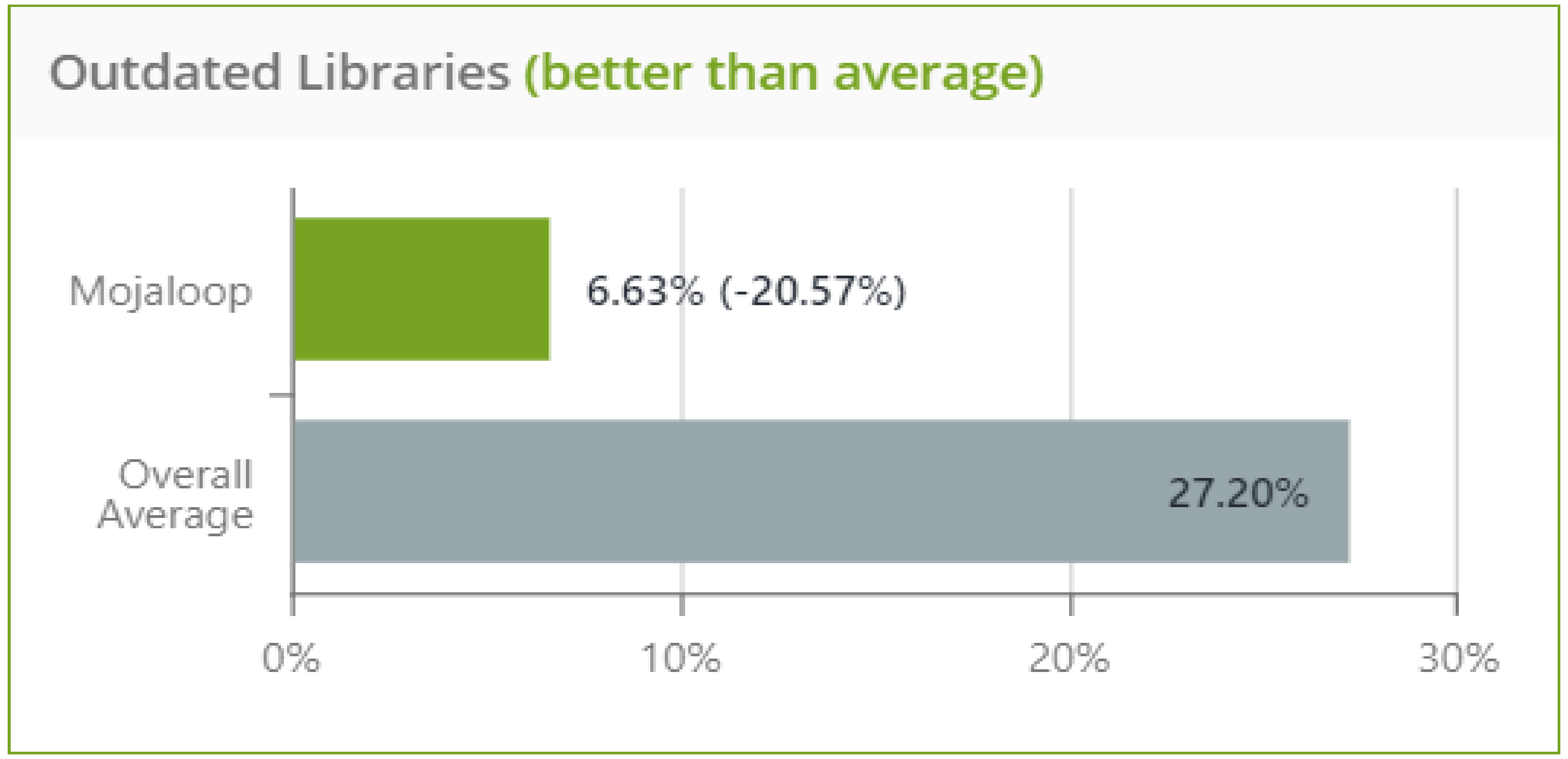
Quarterly OSS Results Comparison

All Mojaloop repos were included in the scan:

18 January 2022	18 April 2022	26 July 2022
104 Codebases with 7055 libraries	**111 Codebases with 7729 libraries**	**119 Codebases with 8461 libraries**
• **6625** libraries are up to date – Excellent version management • **430** libraries are outdated and should be reviewed for upgrades • **130** libraries with multiple version and should be upgraded to the most updated version	• **7221** libraries are up to date – Excellent version management • **489** libraries are outdated and should be reviewed for upgrades • **165** libraries with multiple version and should be upgraded to the most updated version	• **7881** libraries are up to date – Excellent version management • **561** libraries are outdated and should be reviewed for upgrades • **167** libraries with multiple version and should be upgraded to the most updated version

According to WhiteSource Benchmark database as of 26 July 22, Mojaloop is better than average in both vulnerable and outdated libraries.


Vulnerable Libraries (better than average)


Outdated Libraries (better than average)

PI 19 Objectives

1. Quarterly OSS scan

2. DevSecOps maintenance
   a. Regular security patches + updates
   b. Vulnerability management program and support to implementers
   c. Continue to refine DevOps policies to prevent against dependency attacks

3. DevSecOps
   - Approve the Code Signing Design and Implement it on helm
   - Finalize the code security standards based on the draft framework
   - Implement a static code analysis tool

4. Product strategy alignment
   - Consistent messaging on security and compliance matters
   - Response to open questions from prospective adopters and current implementation teams

muchas gracias

COMMUNITY

mojaloop

MEETING

Thank you

Questions and comments