Tanzu

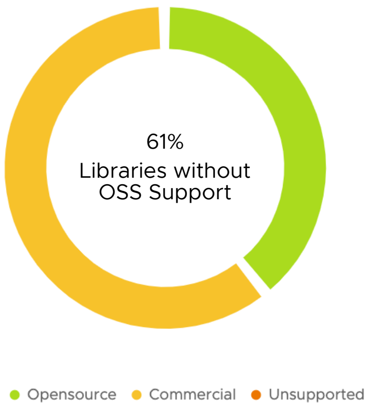
Spring Health Assessment

Created on Apr 08, 2024

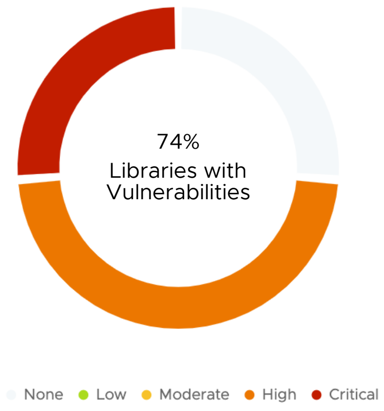
23

Total Spring libraries used

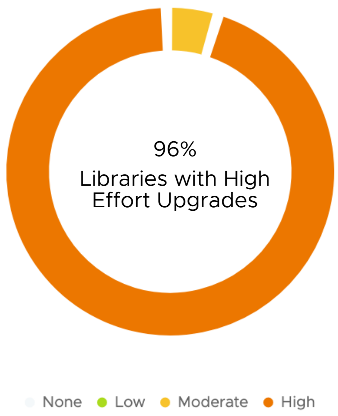
OSS Support Status



Security Vulnerabilities



Upgrade Effort



Findings

Your percentage of supported libraries will reduce from **39%** to **0%** over the next 4 months.

You have **17 libraries** with security vulnerabilities.

22 of you libraries are likely to require **High engineering effort** to upgrade.

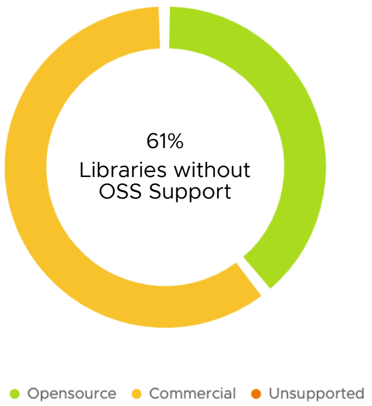
Recommendations

Purchase Spring Runtime to extend your support until **Apr 08, 2025**, for **23 libraries** which are set to expire in **4 months**.

Upgrade **17 libraries** with identified vulnerabilities.

Questions? Get help from Tanzu Labs to upgrade your apps.

OSS Support Status



9

Opensource

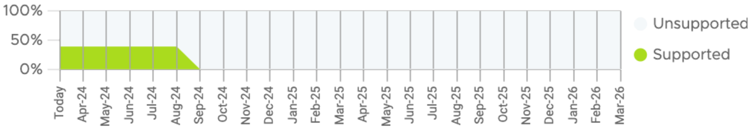
14

Commercial

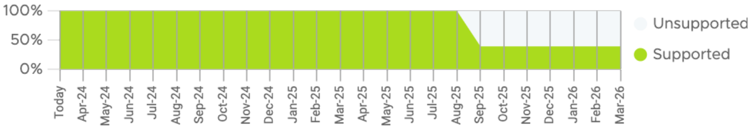
0

Unsupported

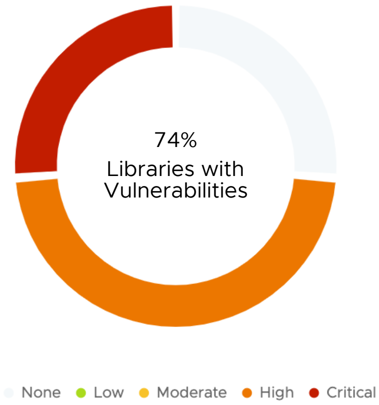
OSS Support Status Over Time



Tanzu Spring Runtime Support Status Over Time



Security Vulnerabilities



6
Critical

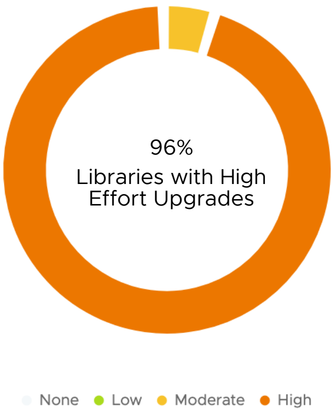
11
High

0
Moderate

0
Low

6
None

Upgrade Effort



22
High

1
Moderate

0
Low

Get Help

Elevate your development with exclusive enterprise features and commercial Spring support

Discover the power of VMware Tanzu Spring Runtime. Benefit from 24x7 support for the entire Spring ecosystem, and get packaged versions of popular projects tailored for seamless integration with Kubernetes—all built by the core Spring engineering team.

Learn more

Own your modernization journey

VMware Tanzu Spring Consulting (formerly Pivotal Labs) partners with organizations worldwide to accelerate the delivery of software and modernize legacy apps, while reducing operating costs and risk.

Learn more

Run Spring Health Assessment across your portfolio & upgrade to SpringBoot 3 automatically

Join the Spring Design Partner Program to use the Spring Health Assessment on a larger scale and automatically upgrade your Spring libraries and APIs to the latest versions minimizing the amount of breaking changes. Simply reach out to shar-sdp.PDL@broadcom.com before the 16th of February 2024 to request access to the program.

Learn more

Libraries

Sort by: Support

org.springframework.boot:spring-boot:2.7.1

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	3	HIGH	SUPPORTED	HIGH

Vulnerabilities

Vulnerability	Status	Transitive dependency	CVE
Spring Framework vulnerable to denial of service	HIGH	YES	CVE-2023-20863
Spring Boot denial of service vulnerability	MODERATE	NO	CVE-2023-34055
Spring Framework vulnerable to denial of service via specially crafted SpEL expression	MODERATE	YES	CVE-2023-20861

Upgrade Plan

Upgrade Step	Effort
Upgrade spring-boot from 2.7.x to 3.2.x	HIGH

org.springframework.boot:spring-boot-autoconfigure:2.7.1

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	4	HIGH	SUPPORTED	HIGH

org.springframework.boot:spring-boot-starter-tomcat:2.7.1

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	6	HIGH	SUPPORTED	HIGH

org.springframework.boot:spring-boot-actuator:2.7.1

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	3	HIGH	SUPPORTED	HIGH

io.micrometer:micrometer-core:1.9.1

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	0	NONE	SUPPORTED	MEDIUM

org.springframework.boot:spring-boot-starter-web:2.7.1

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	23	CRITICAL	SUPPORTED	HIGH

org.springframework.boot:spring-boot-starter:2.7.1

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	12	HIGH	SUPPORTED	HIGH

org.springframework.boot:spring-boot-actuator-autoconfigure:2.7.1 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	7	❗ CRITICAL	⚠ SUPPORTED	❗ HIGH

org.springframework.boot:spring-boot-starter-logging:2.7.1 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	1	❗ HIGH	⚠ SUPPORTED	❗ HIGH

org.springframework.boot:spring-boot-test-autoconfigure:2.7.1 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	4	❗ HIGH	⚠ SUPPORTED	❗ HIGH

org.springframework.boot:spring-boot-test:2.7.1 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	3	❗ HIGH	⚠ SUPPORTED	❗ HIGH

org.springframework.boot:spring-boot-starter-actuator:2.7.1 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	15	❗ CRITICAL	⚠ SUPPORTED	❗ HIGH

org.springframework.boot:spring-boot-starter-json:2.7.1 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	17	❗ CRITICAL	⚠ SUPPORTED	❗ HIGH

org.springframework.boot:spring-boot-starter-test:2.7.1 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2023-11-24	2025-08-24	14	❗ HIGH	⚠ SUPPORTED	❗ HIGH

org.springframework:spring-core:5.3.21 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2024-08-31	2026-12-31	0	✓ NONE	✓ SUPPORTED	❗ HIGH

org.springframework:spring-expression:5.3.21 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2024-08-31	2026-12-31	2	❗ HIGH	✓ SUPPORTED	❗ HIGH

org.springframework:spring-aop:5.3.21 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2024-08-31	2026-12-31	0	✓ NONE	✓ SUPPORTED	❗ HIGH

org.springframework:spring-test:5.3.21 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2024-08-31	2026-12-31	0	✓ NONE	✓ SUPPORTED	❗ HIGH

org.springframework:spring-webmvc:5.3.21 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2024-08-31	2026-12-31	5	❗ CRITICAL	✅ SUPPORTED	❗ HIGH

org.springframework:spring-jcl:5.3.21 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2024-08-31	2026-12-31	0	✅ NONE	✅ SUPPORTED	❗ HIGH

org.springframework:spring-beans:5.3.21 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2024-08-31	2026-12-31	0	✅ NONE	✅ SUPPORTED	❗ HIGH

org.springframework:spring-context:5.3.21 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2024-08-31	2026-12-31	2	❗ HIGH	✅ SUPPORTED	❗ HIGH

org.springframework:spring-web:5.3.21 +

OSS support ends	Commercial support ends	Vulnerabilities	Vulnerability status	Support status	Effort
2024-08-31	2026-12-31	3	❗ CRITICAL	✅ SUPPORTED	❗ HIGH

Understanding Effort & Support Levels

Effort

❗ HIGH

Requires extensive refactoring for dependency upgrades.

⚠️ MODERATE

Needs some manual updates due to major changes in dependencies.

⚠️ LOW

Simple version update, no significant code changes.

Support

✅ SUPPORTED

Currently under open-source support.

⚠️ SUPPORTED

Under commercial support, with extended updates for Tanzu customers.

❗ UNSUPPORTED

No longer supported, no updates available.

Disclaimer and Known Limitations

Please Read Carefully

This report provides an assessment of the Spring libraries used within your project, detailing support status, security vulnerabilities, and migration efforts. It is essential to understand the scope and limitations of this assessment:

- Our vulnerabilities database is updated every 3 hours. If a new vulnerability appears over that period, it will not be included in the report.
- The vulnerabilities introduced by transitive dependencies do not consider overridden versions through dependency management.
- The vulnerabilities introduced by optional transitive dependencies are not considered.
- You do not always require full upgrade to mitigate the vulnerabilities reflected in the report. Sometimes, you can alternatively overwrite a dependency.
- Projects with N/A dates include projects that are run by the community or are not yet supported by the Spring team.
- This service is still in BETA, which means that we can not guarantee a 99.5 availability.

Should you encounter any issues or anomalies in this report not listed above, we strongly encourage you to contact our support team for a detailed review and assistance in UTC+1 working hours.

Support Contact

Email: shar-support.PDL@broadcom.com

For support, reach out to us through the contact options above, and we will be glad to assist you during working hours.