Red Hat build of Apache Camel for Spring Boot 3.20

Release Notes for Red Hat build of Apache Camel for Spring Boot 3.20

What's new in Red Hat build of Apache Camel for Spring Boot

Last Updated: 2024-02-16

Red Hat build of Apache Camel for Spring Boot 3.20 Release Notes for Red Hat build of Apache Camel for Spring Boot 3.20

What's new in Red Hat build of Apache Camel for Spring Boot

Legal Notice

Abstract

Describes the Red Hat build of Apache Camel for Spring Boot product and provides the latest details on what's new in this release.

Table of Contents

CHAPTER 1. CAMEL SPRING BOOT RELEASE NOTES

1.1. CAMEL SPRING BOOT FEATURES

Camel Spring Boot introduces Camel support for Spring Boot which provides auto-configuration of the Camel and starters for many Camel components. The opinionated auto-configuration of the Camel context auto-detects Camel routes available in the Spring context and registers the key Camel utilities (like producer template, consumer template and the type converter) as beans.

1.2. SUPPORTED PLATFORMS, CONFIGURATIONS, DATABASES, AND EXTENSIONS FOR CAMEL SPRING BOOT

- For information about supported platforms, configurations, and databases in Camel Spring Boot, see the Supported Configuration page on the Customer Portal (login required).
- For a list of Red Hat Camel Spring Boot extensions, see the *Camel Spring Boot Reference* (login required).

1.3. IMPORTANT NOTES

Documentation for Camel Spring Boot components is available in the Camel Spring Boot Reference. Documentation for additional Camel Spring Boot components will be added to this reference guide.

Migration from Fuse 7.11 to Camel Spring Boot

This release contains a Migration Guide documenting the changes required to successfully run and deploy Fuse 7.11 applications on Camel Spring Boot. It provides information on how to resolve deployment and runtime problems and prevent changes in application behavior. Migration is the first step in moving to the Camel Spring Boot platform. Once the application deploys successfully and runs, users can plan to upgrade individual components to use the new functions and features of Camel Spring Boot.

Support for EIP circuit breaker

The Circuit Breaker EIP for Camel Spring Boot supports Resilience4j configuration. This configuration provides integration with Resilience4j to be used as Circuit Breaker in Camel routes.

Technology Preview extensions

The following extensions are supported as Technology Preview for CSB 3.20 release version.

- camel-spring-batch-starter
- camel-spring-jdbc-starter
- camel-spring-ldap-starter
- camel-spring-rabbitmq-starter
- camel-spring-redis-starter
- camel-spring-security-starter
- camel-spring-ws-starter

1.4. CAMEL SPRING BOOT FIXED ISSUES

The following sections list the issues that have been fixed in Camel Spring Boot.

1.4.1. Camel Spring Boot version 3.20.5 Fixed Issues

The following table lists the resolved bugs in Camel Spring Boot version 3.20.5

Table 1.1. Camel Spring Boot version 3.20.5 Resolved Bugs

Issue	Description
CSB-3313	CVE-2023-51074 json-path: stack-based buffer overflow in Criteria.parse method

1.4.2. Camel Spring Boot version 3.20.4 Fixed Issues

The following table lists the resolved bugs in Camel Spring Boot version 3.20.4.

Table 1.2. Camel Spring Boot version 3.20.4 Resolved Bugs

Issue	Description
CSB-2942	CVE-2023-5072 JSON-java: parser confusion leads to OOM

1.4.3. Camel Spring Boot version 3.20.3 Fixed Issues

The following table lists the resolved bugs in Camel Spring Boot version 3.20.3

Table 1.3. Camel Spring Boot version 3.20.3 Resolved Bugs

Issue	Description
CSB-2688	CVE-2023-44487 netty-codec-http2: HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack)
CSB-2694	CVE-2023-44487 undertow: HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack)

1.4.4. Camel Spring Boot version 3.20.2 Fixed Issues

The following table lists the resolved bugs in Camel Spring Boot version 3.20.2

Table 1.4. Camel Spring Boot version 3.20.2 Resolved Bugs

Issue	Description
CSB-2340	CVE-2023-20873 spring-boot: Security Bypass With Wildcard Pattern Matching on Cloud Foundry [rhint-camel-spring-boot-3.20]
CSB-2350	CVE-2023-34455 snappy-java: Unchecked chunk length leads to DoS [rhint-camel-spring-boot-3.20]

1.4.5. Camel Spring Boot version 3.20.1 Update 1 Fixed Issues

The following table lists the resolved bugs in Camel Spring Boot version 3.20.1 Update 1.

Table 1.5. Camel Spring Boot version 3.20.1 Update 1 Resolved Bugs

Issue	Description
CSB-1524	CVE-2022-31690 spring-security-oauth2-client: Privilege Escalation in spring-security-oauth2-client [rhint-camel-spring-boot-3]
CSB-1718	CVE-2023-20883 spring-boot: Spring Boot Welcome Page DoS Vulnerability [rhint-camel-spring-boot-3.20]
CSB-1719	CVE-2023-24815 vertx-web: StaticHandler disclosure of classpath resources on Windows when mounted on a wildcard route [rhint-camel-spring-boot-3.20]
CSB-1760	CXF TrustedAuthorityValidatorTest failure
CSB-1821	Backport CAMEL-19421 - Camel-Jira: Use Files.createTempFile in FileConverter instead of creating File directly

1.4.6. Camel Spring Boot version 3.20 Fixed Issues

The following table lists the resolved bugs in Camel Spring Boot version 3.20.

Table 1.6. Camel Spring Boot version 3.20 Resolved Bugs

Issue	Description
CSB-656	CVE-2022-25857 snakeyaml: Denial of Service due to missing nested depth limitation for collections [rhint-camel-spring-boot-3]
CSB-699	CVE-2022-40156 xstream: Xstream to serialise XML data was vulnerable to Denial of Service attacks [rhint-camel-spring-boot-3]

Issue	Description
CSB-702	CVE-2022-40152 woodstox-core: woodstox to serialise XML data was vulnerable to Denial of Service attacks [rhint-camel-spring-boot-3]
CSB-703	CVE-2022-40151 xstream: Xstream to serialise XML data was vulnerable to Denial of Service attacks [rhint-camel-spring-boot-3]
CSB-714	CVE-2022-38752 snakeyaml: Uncaught exception in java.base/java.util.ArrayList.hashCode [rhint-camel-spring-boot-3]
CSB-715	CVE-2022-38751 snakeyaml: Uncaught exception in java.base/java.util.regex.Pattern$Ques.match [rhint-camel-spring-boot-3]
CSB-716	CVE-2022-38750 snakeyaml: Uncaught exception in org.yaml.snakeyaml.constructor.BaseConstructor.constructObject [rhint-camel-spring-boot-3]
CSB-717	CVE-2022-38749 snakeyaml: Uncaught exception in org.yaml.snakeyaml.composer.Composer.composeSequenceNode [rhint-camel-spring-boot-3]
CSB-719	CVE-2022-42003 jackson-databind: deep wrapper array nesting wrt UNWRAP_SINGLE_VALUE_ARRAYS [rhint-camel-spring-boot-3]
CSB-720	CVE-2022-42004 jackson-databind: use of deeply nested arrays [rhint-camel-spring-boot-3]
CSB-721	CVE-2022-41852 JXPath: untrusted XPath expressions may lead to RCE attack [rhint-camel-spring-boot-3]
CSB-722	CVE-2022-41853 hsqldb: Untrusted input may lead to RCE attack [rhint-camel-spring-boot-3]
CSB-751	CVE-2022-33681 org.apache.pulsar-pulsar-client: Apache Pulsar: Improper Hostname Verification in Java Client and Proxy can expose authentication data via MITM [rhint-camel-spring-boot-3]
CSB-794	CVE-2022-40150 jettison: memory exhaustion via user-supplied XML or JSON data [rhint-camel-spring-boot-3]
CSB-811	CVE-2022-39368 scandium: Failing DTLS handshakes may cause throttling to block processing of records [rhint-camel-spring-boot-3]
CSB-813	CVE-2022-31777 apache-spark: XSS vulnerability in log viewer UI Javascript [rhint-camel-spring-boot-3]
CSB-819	camel-kafka-starter: KafkaConsumerHealthCheckIT is not working

Issue	Description
CSB-820	I2x6 cq-maven-plugin setting wrong version for camel-avro-rpc-component
CSB-851	camel-cxf-rest-starter: EchoService is not an interface error on JDK 17
CSB-852	camel-infinispan-starter : tests fail on FIPS enabled environment
CSB-883	CVE-2022-37866 apache-ivy: : Apache Ivy: Ivy Path traversal [rhint-camel-spring-boot-3]
CSB-904	CVE-2022-41881 codec-haproxy: HAProxyMessageDecoder Stack Exhaustion DoS [rhint-camel-spring-boot-3]
CSB-905	CVE-2022-41854 dev-java-snakeyaml: dev-java/snakeyaml: DoS via stack overflow [rhint-camel-spring-boot-3]
CSB-906	[archetype] OMP version in openshift profile
CSB-929	CVE-2022-38648 batik: Server-Side Request Forgery [rhint-camel-spring-boot-3]
CSB-930	CVE-2022-38398 batik: Server-Side Request Forgery [rhint-camel-spring-boot-3]
CSB-931	CVE-2022-40146 batik: Server-Side Request Forgery (SSRF) vulnerability [rhint-camel-spring-boot-3]
CSB-942	CVE-2022-4492 undertow: Server identity in https connection is not checked by the undertow client [rhint-camel-spring-boot-3]
CSB-1203	CVE-2022-45047 sshd-common: mina-sshd: Java unsafe deserialization vulnerability
CSB-1239	SAP quickstart spring-boot examples have circular references
CSB-1242	The camel-salesforce-maven-plugin:3.20.1 fails when running with openJDK11 in FIPS mode
CSB-1274	CVE-2021-37533 apache-commons-net: FTP client trusts the host from PASV response by default [rhint-camel-spring-boot-3]
CSB-1334	CVE-2023-24998 tomcat: Apache Commons FileUpload: FileUpload DoS with excessive parts [rhint-camel-spring-boot-3]
CSB-1335	CVE-2022-41966 xstream: Denial of Service by injecting recursive collections or maps based on element's hash values raising a stack overflow [rhint-camel-spring-boot-3]

Issue	Description
CSB-1373	FIPS-mode: Invalid algorythms & security issues on some camel components
CSB-1404	The Spring Boot version is wrong in the BOM
CSB-1436	CVE-2023-20860 springframework: Security Bypass With Un-Prefixed Double Wildcard Pattern [rhint-camel-spring-boot-3]
CSB-1437	CVE-2023-20861 springframework: Spring Expression DoS Vulnerability [rhint-camel-spring-boot-3]
CSB-1441	CVE-2022-42890 batik: Untrusted code execution in Apache XML Graphics Batik [rhint-camel-spring-boot-3]
CSB-1442	CVE-2022-41704 batik: Apache XML Graphics Batik vulnerable to code execution via SVG [rhint-camel-spring-boot-3]
CSB-1443	CVE-2022-37865 apache-ivy: Directory Traversal [rhint-camel-spring-boot-3]
CSB-1444	CVE-2023-22602 shiro-core: shiro: Authentication bypass through a specially crafted HTTP request [rhint-camel-spring-boot-3]
CSB-1482	CVE-2023-1436 jettison: Uncontrolled Recursion in JSONArray [rhint-camel-spring-boot-3]
CSB-1499	Classes generated by camel-openapi-rest-dsl-generator are not added to jar
CSB-1533	[cxfrs-component] camel-cxf-rest-starter needs cxf-spring-boot-autoconfigure
CSB-1536	CVE-2023-20863 springframework: Spring Expression DoS Vulnerability [rhint-camel-spring-boot-3.14]
CSB-1540	CVE-2023-1370 json-smart: Uncontrolled Resource Consumption vulnerability in json-smart (Resource Exhaustion) [rhint-camel-spring-boot-3.18]

1.5. ADVISORIES RELATED TO THIS RELEASE

The following advisories have been issued to document enhancements, bugfixes, and CVE fixes included in this release.

- RHSA-2023:7845
- RHSA-2023:6079

- RHSA-2023:5148

1.6. ADDITIONAL RESOURCES

- Supported Configurations
- Camel Spring Boot Reference
- Getting Started with Camel Spring Boot
- Migration Guide