

Jasper Server OS 10.0.4 Patch Notes

Table of Content

JASPER SERVER OS	2
NEW FEATURES (CUMULATIVE SINCE VERSION 10.0.0)	2
BUG FIXES VERION 10.0.1	2
BUG FIXES VERION 10.0.2	2
BUG FIXES VERION 10.0.3	2
SECURITY FIXES VERSION 10.0.4	3

JASPER SERVER OS

10.0.0 pulls Jasper Server OS through the Jakarta migration, allowing deployment on new application servers and enabling further security updates. A very useful upgrade is supporting Jasper Reports written for versions 6 and 7 of the JR library, allowing easy migrations from JRS 8.4.x and earlier versions.

For full update documentation please refer to 10.0.0 Release Notes.

NEW FEATURES (CUMULATIVE SINCE VERSION 10.0.0)

- Docker image: Tomcat's JAVA_OPTS can now be modified by passing the environment variable JAVA_OPTS_APPEND to the container. It is not written to a file, but read from the environment each time, so it can/must also be set each time a container starts up.
- JRS compensates for a bug in JSS < 7.0.6 related to the one we fixed in JRS 10.0.2, in which elements of Scatter and other XY-based charts are wrongly serialized and the resulting JRXML cannot be parsed. JRS corrects these properties in JRXMLv7 files.

BUG FIXES VERION 10.0.1

- Fixed a bug where charts Jasper Reports version 6 reports could not be executed if certain properties of the axis formats were set
- Fixed a problem with SMTP configuration for scheduled reports - scheduled reports can now send mail notifications normally
- Fixed an error in buildomatic (command line) import/export on Linux. Previously, only GUI imports worked
- Fixed an error when importing schedules with buildomatic (command line)

BUG FIXES VERION 10.0.2

- Fixed a problem where the installer would crash if DB password encryption was activated. Encryption can be enabled in the Docker image by passing
`-e ENCRYPT_DB_PASSWORD=true.`
- Fixed a problem where the installer would crash on Java 21
- Fixed a problem compiling version 6.x Jasper Reports with scatter and other XY-based charts
- Fixed a problem compiling version 6.x Jasper Reports with charts if item labels' font size was set

BUG FIXES VERION 10.0.3

- Fixed a bug where named scriptlets would cause a report to crash because the corresponding parameter could not be generated

SECURITY FIXES VERSION 10.0.4

Known Issues as of: 2026-09-30

FRONTEND

Issue	Code	Description
HIGH		
CVE-2024-38999	requirejs (2.3.6)	Library Update to version 2.3.8
CVE-2026-27601	underscore (1.13.1)	Library Update to version 1.13.8
CVE-2026-4800	lodash (4.17.21)	Library Update to version 4.18.0
MODERATE		
CVE-2025-13465	lodash (4.17.21)	Library Update to version 4.18.0
CVE-2025-27789	@babel/runtime (7.12.13, 7.12.5, 7.13.9)	Library Update to version 7.26.10
CVE-2025-27789	@babel/runtime-corejs2 (7.6.0)	Library Update to version 7.26.10
CVE-2026-2950	lodash (4.17.21)	Library Update to version 4.18.0

BACKEND

Issue	Code	Description
CRITICAL		
CVE-2019-13990	quartz-commonj-2.1.7.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2023-39017	quartz-2.3.2.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2023-39017	quartz-commonj-2.1.7.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2024-1597	postgresql-42.5.4.jar	Library Update to version 42.7.12
CVE-2024-22949	jfreechart-1.5.4.jar	Library Update to version 1.5.6

Issue	Code	Description
CVE-2026-33117	azure-core-0.7.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2026-41409	mina-core-2.1.10.jar	Library Update to version 2.1.12
CVE-2026-41635	mina-core-2.1.10.jar	Library Update to version 2.1.12
CVE-2026-41855	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-42778	mina-core-2.1.10.jar	Library Update to version 2.1.12
CVE-2026-42779	mina-core-2.1.10.jar	Library Update to version 2.1.12
CVE-2026-48144	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-55971	libthrift-0.14.1.jar	Library Update to version 0.24.0
HIGH		
CVE-2018-1258	spring-security-core-6.5.9.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2018-1258	spring-security-ldap-6.5.9.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2018-1258	spring-security-web-6.5.9.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2020-25638	hibernate-jmx-3.3.2.GA.jar	Library Update to version 5.4.3
CVE-2022-40152	woodstox-core-6.3.1.jar	Library Update to version 7.0.0
CVE-2022-42003	jackson-databind-2.13.4.jar	Library Update to version 2.18.9
CVE-2023-22551	ftpserver-core-1.0.3.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2023-22551	jasperserver-ftp-9.0.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2023-34453	snappy-java-1.1.2.6.jar	Library Update to version 1.1.10.4
CVE-2023-34454	snappy-java-1.1.2.6.jar	Library Update to version 1.1.10.4
CVE-2023-34455	snappy-java-1.1.2.6.jar	Library Update to version 1.1.10.4

Issue	Code	Description
CVE-2023-43642	snappy-java-1.1.2.6.jar	Library Update to version 1.1.10.4
CVE-2023-49735	tiles-core-3.1.0.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2023-49735	tiles-extras-3.1.0.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2023-52070	jfreechart-1.5.4.jar	Library Update to version 1.5.6
CVE-2024-21634	ion-java-1.0.2.jar	Removed unused transitive dependency from AWS SDK modules.
CVE-2024-23076	jfreechart-1.5.4.jar	Library Update to version 1.5.6
CVE-2024-23077	jfreechart-1.5.4.jar	Library Update to version 1.5.6
CVE-2024-29131	commons-configuration2-2.8.0.jar	Library Update to version 2.10.1
CVE-2024-29131	commons-configuration2-2.9.0.jar	Library Update to version 2.10.1
CVE-2025-27553	commons-vfs-1.0.jar	Library Update to version 2.10.0
CVE-2025-48431	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2025-48734	commons-beanutils-1.9.4.jar	Library Update to version 1.11.0
CVE-2025-48976	commons-fileupload-1.5.jar	Library Update to version 1.6.0
CVE-2025-5222	icu4j-57.1.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2026-24051	opentelemetry-api-1.31.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2026-39883	opentelemetry-api-1.31.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2026-39883	opentelemetry-extension-annotations-1.18.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2026-41602	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-41604	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-41605	libthrift-0.14.1.jar	Library Update to version 0.24.0

Issue	Code	Description
CVE-2026-41608	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-41636	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-41838	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41842	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41848	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41850	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41851	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-42198	postgresql-42.5.4.jar	Library Update to version 42.7.12
CVE-2026-43869	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-43870	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-43871	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-48145	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-48586	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-49158	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-54512	jackson-databind-2.13.4.jar	Library Update to version 2.18.9
CVE-2026-54512	jackson-databind-2.16.0.jar	Library Update to version 2.18.9
CVE-2026-54513	jackson-databind-2.13.4.jar	Library Update to version 2.18.9
CVE-2026-54513	jackson-databind-2.16.0.jar	Library Update to version 2.18.9
CVE-2026-55968	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-55969	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-58389	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-58662	libthrift-0.14.1.jar	Library Update to version 0.24.0
MODERATE		
CVE-2019-14900	hibernate-jmx-3.3.2.GA.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2023-35116	jackson-databind-2.13.4.jar	Library Update to version 2.18.9

Issue	Code	Description
CVE-2024-29133	commons-configuration2-2.8.0.jar	Library Update to version 2.10.1
CVE-2024-29133	commons-configuration2-2.9.0.jar	Library Update to version 2.10.1
CVE-2025-30474	commons-vfs-1.0.jar	Library Update to version 2.10.0
CVE-2026-22740	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-22745	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-39882	opentelemetry-api-1.31.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2026-39882	opentelemetry-extension-annotations-1.18.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2026-41178	opentelemetry-api-1.31.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2026-41178	opentelemetry-extension-annotations-1.18.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2026-41606	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-41607	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-41839	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41840	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41841	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41843	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41844	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41845	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41846	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41852	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41853	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-41854	spring-core-6.2.17.jar	Library Update to version 6.2.19
CVE-2026-43868	libthrift-0.14.1.jar	Library Update to version 0.24.0

Issue	Code	Description
CVE-2026-44967	opentelemetry-extension-annotations-1.18.0.jar	The attack scenario described in this CVE is not applicable to JasperServer OS. Therefore, the CVE has been excluded.
CVE-2026-45205	commons-configuration2-2.8.0.jar	Library Update to version 2.10.1
CVE-2026-45205	commons-configuration2-2.9.0.jar	Library Update to version 2.10.1
CVE-2026-50193	jackson-databind-2.13.4.jar	Library Update to version 2.18.9
CVE-2026-54514	jackson-databind-2.13.4.jar	Library Update to version 2.18.9
CVE-2026-54514	jackson-databind-2.16.0.jar	Library Update to version 2.18.9
CVE-2026-54515	jackson-databind-2.13.4.jar	Library Update to version 2.18.9
CVE-2026-54515	jackson-databind-2.16.0.jar	Library Update to version 2.18.9
CVE-2026-55970	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-58023	libthrift-0.14.1.jar	Library Update to version 0.24.0
CVE-2026-66053	libthrift-0.14.1.jar	Library Update to version 0.24.0
LOW		
CVE-2026-22741	spring-core-6.2.17.jar	Library Update to version 6.2.19