Liberica JDK 11.0.31+11
Release Notes

Liberica JDK
11.0.31
April 21, 2026

bellsoft

Copyright © BellSoft Corporation 2018-2026.

BellSoft software contains open source software. Additional information about third party code is available at https://bell-sw.com/third_party_licenses. You can also get more information on how to get a copy of source code by contacting info@bell-sw.com.

THIS INFORMATION MAY CHANGE WITHOUT NOTICE. TO THE EXTENT PERMITTED BY APPLICABLE LAW, BELLSOFT PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BELLSOFT BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BELLSOFT IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in this document is governed by the applicable license agreement, which is not modified in any way by the terms of this notice.

Alpaquita, Liberica and BellSoft are trademarks or registered trademarks of BellSoft Corporation. The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis. Java and OpenJDK are trademarks or registered trademarks of Oracle and/or its affiliates. Other trademarks are the property of their respective owners and are used only for identification purposes.

Contents

1. Version information 5

2. What’s New 6

Notable Changes 6

Graal support in Liberica JDK 11 8

IANA TZ Data version 8

Briefly 8

Changes to past timestamps 8

Changes to build procedure 8

Changes to code 8

Changes to commentary 9

3. Known Issues 10

4. Fixed CVEs 11

5. Resolved Issues 12

JDK issues 12

JFX issues 16

6. Updates to Third Party Libraries 18

7. Upgrading to the New Version 19

1. Version information

This document provides information about Liberica JDK 11.0.31 release. The full version string for this update release is 11.0.31+11. The version number is 11.

Liberica JDK 11 is distributed as `.apk`, `.rpm`, `.zip`, `.deb`, `.pkg`, and `.tar.gz` packages. Please select the most appropriate for your purposes.

2. What's New

This release contains the following updates and new features.

Notable Changes

This is the list of the notable issues fixed in this release.

Issue ID	
JDK-8340321	Summary: Disabled SHA-1 in TLS 1.2 and DTLS 1.2 Handshake Signatures Description: The SHA-1 algorithm has been disabled by default in TLS 1.2 and DTLS 1.2 handshake signatures, by adding `rsa_pkcs1_sha1 usage HandshakeSignature, ecdsa_sha1 usage HandshakeSignature, dsa_sha1 usage HandshakeSignature` to the `jdk.tls.disabledAlgorithms` security property in the `java.security` config file. RFC 9155 deprecates the use of SHA-1 in TLS 1.2 and DTLS 1.2 digital signatures. Users can, at their own risk, re-enable the SHA-1 algorithm in TLS 1.2 and DTLS 1.2 handshake signatures by removing `rsa_pkcs1_sha1 usage HandshakeSignature, ecdsa_sha1 usage HandshakeSignature, dsa_sha1 usage HandshakeSignature` from the `jdk.tls.disabledAlgorithms` security property.

Issue ID	
JDK-8349583	Summary: Mechanism to Disable Signature Schemes Based on Their TLS Scope Description: TLS protocol specific usage constraints are now supported by the `jdk.tls.disabledAlgorithms` property in the `java.security` configuration file. `HandshakeSignature` restricts the use of an algorithm in TLS handshake signatures. `CertificateSignature` restricts the use of an algorithm in certificate signatures. An algorithm with this constraint cannot include other usage types defined in the `jdk.certpath.disabledAlgorithms` property. The usage type follows the keyword and more than one usage type can be specified with a whitespace delimiter.
JDK-8369282	Summary: Distrust TLS server certificates anchored by Chunghwa ePKI Root CA Description: TLS server certificates anchored by the Chunghwa root CAs are distrusted or distrusted after a specific date by Google and Mozilla. The restrictions will be enforced in the SunJSSE Provider of the Java Secure Socket Extension (JSSE) API. A TLS session will not be negotiated if the server's certificate chain is anchored by any of the mentioned Certificate Authorities and the certificate's notBefore date is after March 17, 2026. An application will receive an Exception with a message indicating the trust anchor (root) is not trusted.
JDK-8373476	Summary: Update Timezone Data to 2025c Description: The 2025c release of the tz code and data is available. This release mostly changes code and commentary. The only changed data are leap second table expiration and pre-1976 time in Baja California. This release contains several code changes for compatibility with FreeBSD.

Graal support in Liberica JDK 11

Liberica JDK continues to provide support for AOT and Graal JIT. Since in OpenJDK 11 builds these features are deemed experimental and deprecated, it is recommended to compile native executables with Liberica Native Image Kit to avoid errors.

IANA TZ Data version

This release of Liberica JDK 11.0.31 comes with the 2025c version of the in-tree copy of the IANA timezone database. The following are the key features of this version.

This release mostly changes code and commentary. The only changed data are leap second table expiration and pre-1976 time in Baja California.

Briefly

Several code changes for compatibility with FreeBSD.

Changes to past timestamps

Baja California agreed with California's DST rules in 1953 and in 1961 through 1975, instead of observing standard time all year.

Changes to build procedure

Files in distributed tarballs now have correct commit times. Formerly, the committer's time zone was incorrectly ignored.

Changes to code

An unset TZ is no longer invalid when `/etc/localtime` is missing, and is abbreviated "UTC" not "-00". This reverts to 2024b behavior.

New function `offtime_r`, short for `fixed-offset localtime_rz`. It is defined if `STD_INSPIRED` is defined.

Changes to commentary

The `leapseconds` file contains commentary about the `IERS` and `NIST` last-modified and expiration timestamps for leap second data.

For more information, see JDK-8373476.

3. Known Issues

This release does not contain any known issues.

4. Fixed CVEs

This is the list of the security issues fixed in this release. CVSS scores are provided using the CVSS version 3.1 scoring system.

CVE ID	CVSS score	Component	Module	Attack Vector	Complexity	Privileges	User Interaction	Scope	Confidentiality	Integrity	Availability
CVE-2026-20652	7.5	javafx	web	network	low	none	none	unchanged	none	none	high
CVE-2026-22007	2.9	security-libs	java.security	local	high	none	none	unchanged	low	none	none
CVE-2026-22013	5.3	security-libs	org.ietf.jgss	network	high	none	required	unchanged	high	none	none
CVE-2026-22016	7.5	xml	jaxp	network	low	none	none	unchanged	high	none	none
CVE-2026-22018	3.7	core-libs	java.util	network	high	none	none	unchanged	none	none	low
CVE-2026-22021	5.3	security-libs	java.security	network	low	none	none	unchanged	none	none	low
CVE-2026-23865	5.3	client-libs	2d	local	low	none	required	unchanged	low	low	low
CVE-2026-34268	2.9	security-libs	java.security	local	high	none	none	unchanged	low	none	none
CVE-2026-34282	7.5	core-libs	java.net	network	low	none	none	unchanged	none	none	high

5. Resolved Issues

JDK issues

This is the list of general JDK issues fixed in this release.

Issue ID	Summary
JDK-8209362	sun/security/ssl/SSLSocketImpl/ReuseAddr.java failed due to "BindException: Address already in use (Bind failed)"
JDK-8224796	C code is not compiled correctly due to undefined "i386"
JDK-8231449	HttpClient's client ssl certificate authentication seems to be broken
JDK-8263188	JSSE should fail fast if there isn't supported signature algorithm
JDK-8284047	Harmonize/Standardize the SSLSocket/SSLEngine/SSLSocketSSLEngine test templates
JDK-8286694	Incorrect argument processing in java launcher
JDK-8301379	Verify TLS_ECDH_* cipher suites cannot be negotiated
JDK-8303215	Make thread stacks not use huge pages

Issue ID	Summary
JDK-8305186	Reference.waitForReferenceProcessing should be more accessible to tests
JDK-8306014	Update javax.net.ssl TLS tests to use SSLContextTemplate or SSLEngineTemplate
JDK-8306015	Update sun.security.ssl TLS tests to use SSLContextTemplate or SSLEngineTemplate
JDK-8308144	Uncontrolled memory consumption in SSLFlowDelegate.Reader
JDK-8313770	jdk/internal/platform/docker/TestSystemMetrics.java fails on Ubuntu
JDK-8324861	Exceptions::wrap_dynamic_exception() doesn't have ResourceMark
JDK-8336342	Fix known X11 library locations in sysroot
JDK-8336343	Add more known sysroot library locations for ALSA
JDK-8337102	JITTester: Fix breaks in static initialization blocks
JDK-8337669	[17u] Backport of JDK-8284047 missed to delete a file
JDK-8339271	giflib attribution correction
JDK-8340321	Disable SHA-1 in TLS/DTLS 1.2 handshake signatures

Issue ID	Summary
JDK-8342175	MemoryEaterMT fails intermittently with ExceptionInInitializerError
JDK-8343622	AesDkCrypto.stringToKey should not return null
JDK-8345578	New test in JDK-8343622 fails with a promoted build
JDK-8346048	test/lib/containers/docker/DockerRunOptions.java uses addJavaOpts() from ctor
JDK-8348014	Enhance certificate processing
JDK-8349583	Add mechanism to disable signature schemes based on their TLS scope
JDK-8355779	When no "signature_algorithms_cert" extension is present we do not apply certificate scope constraints to algorithms in "signature_algorithms" extension
JDK-8361748	Enforce limits on the size of an XBM image
JDK-8364373	Transform Affine transformations
JDK-8364465	Enhance behavior of some intrinsics
JDK-8364660	ClassVerifier::ends_in_athrow() should be removed
JDK-8366221	[11u] TestPromotionFromSurvivorToTenuredAfterMinorGC.java javac build fails

Issue ID	Summary
JDK-8366817	test/jdk/javax/net/ssl/TLSCommon/interop/JdkProcServer.java and JdkProcClient.java should not delete logs
JDK-8369282	Distrust TLS server certificates anchored by Chunghwa ePKI Root CA
JDK-8369575	Enhance crypto algorithm support
JDK-8370529	Enhance Path Factories Redux
JDK-8370615	Improve Kerberos credentialing
JDK-8370986	Enhance Zip file reading
JDK-8370995	Enhance ZipFile usage
JDK-8371830	Enhance certificate chain validation
JDK-8371935	Enhance key generation
JDK-8372857	Improve debuggability of java/rmi/server/RemoteServer/AddrInUse.java test
JDK-8373254	Bump update version of OpenJDK: 11.0.31
JDK-8373290	Update FreeType to 2.14.1
JDK-8373476	(tz) Update Timezone Data to 2025c
JDK-8373727	New XBM images parser regression: only the first line of the bitmap array is parsed

Issue ID	Summary
JDK-8374213	[11u] [BACKOUT] JDK-8301379 Verify TLS_ECDH_* cipher suites cannot be negotiated
JDK-8374557	Enhance TLS connection handling
JDK-8375057	Update HarfBuzz to 12.3.2
JDK-8375063	Update Libpng to 1.6.54
JDK-8377450	[11u] Tests using Text Blocks fail to compile
JDK-8377526	Update Libpng to 1.6.55
JDK-8379035	(tz) Update Timezone Data to 2026a
JDK-8379158	Update FreeType to 2.14.2
JDK-8379256	Update GIFlib to 6.1.1
JDK-8379424	[11u] Update SSL tests using SSLEngineTemplate
JDK-8380078	Update GIFlib to 6.1.2
JDK-8380959	Update Libpng to 1.6.56
JDK-8382047	Update Libpng to 1.6.57

JFX issues

This is the list of JFX issues fixed in this release.

Issue ID	Summary
JDK-8278021	Fix warnings in macOS glass native code and treat warnings as errors
JDK-8347937	Canvas pattern test fails and crashes on WebKit 620.1
JDK-8368572	Update WebKit to 623.1
JDK-8371052	Update libFFI to 3.5.2
JDK-8374153	Add a MAX_COMPILE_THREADS gradle property to limit number of threads
JDK-8375225	WebIObserverTest fails with WebKit 623.1
JDK-8376282	[linux, macos] JavaFX fails to build WebKit in DebugNative
JDK-8377099	Additional WebKit 623.1 fixes from WebKitGTK 2.50.4
JDK-8377930	Additional WebKit 623.1 fixes from WebKitGTK 2.50.5
JDK-8378034	Add licenses for gcc 14.2.0
JDK-8380557	Additional WebKit 623.1 fixes from WebKitGTK 2.50.6

6. Updates to Third Party Libraries

This is the list of changes in the third party libraries.

Library	Full name	New Version	Module	JBS number
FreeType	FreeType	2.14.2	java.desktop	JDK-8379158
GIFlib	GIFlib	6.1.2	java.desktop	JDK-8380078
HarfBuzz	HarfBuzz	12.3.2	java.desktop	JDK-8375057
Libpng	Libpng	1.6.57	java.awt	JDK-8382047

7. Upgrading to the New Version

To keep your Liberica JDK up-to-date and secure, always upgrade to the newest available version once it is released. To upgrade, install the new version over the previous one. For the installation instructions, see Liberica JDK Installation Guide.

Liberica JDK 11.0.31+11

Release Notes

bell//soft