

Liberica JDK 17.0.21+11

Release Notes



Liberica JDK
17.0.21
October 20, 2026

be//soft

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
Builds of Liberica JDK With CRaC	10
IANA TZ Data version	10
Briefly	10
Changes to future timestamps	10
NOTE FOR 2026b TEMPORARY HACK FOR CLDR AND CANADA	11
Changes to past timestamps	11
Changes to commentary	11

3. Known Issues	12
-----------------	----

4. Fixed CVEs	13
---------------	----

5. Resolved Issues	15
--------------------	----

JDK issues	15
------------	----

JFX issues	29
------------	----

6. Updates to Third Party Libraries	32
-------------------------------------	----

7. Upgrading to the New Version	33
---------------------------------	----

1. Version information

This document provides information about Liberica JDK 17.0.21 release. The full version string for this update release is 17.0.21+11. The version number is 17.

Liberica JDK 17 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-8189441	Summary: Define algorithm names for keys derived from <code>KeyAgreement</code> Description: With the proposed new Key Algorithms section in the Java Security Standard Algorithm Names Specification, the <code>KeyAgreement::generateSecret</code> method is linked to the section to specify the algorithm names that users can provide. Additionally, the potential truncation of the shared secret length to align with the specified algorithm name was clarified. An implementation decides which secret key algorithms from the Key Algorithms section to support and may throw an exception if an unsupported algorithm is specified.

Issue ID

JDK-8298387

Summary: Implement JEP 497: Quantum-Resistant Module-Lattice-Based Digital Signature Algorithm

Description: ML-DSA is a quantum-resistant digital signature algorithm selected by the National Institute of Standards and Technology (NIST) to ensure the security of cryptographic systems in the post-quantum era. ML-DSA is defined and its three standardized parameter sets (ML-DSA-44, ML-DSA-65, and ML-DSA-87) as Java Security Standard Algorithm Names. Implemented `KeyPairGenerator`, `KeyFactory`, and `Signature` implementations of ML-DSA with these standardized parameter set in the SUN security provider. Created new `NamedParameterSpec` constants for ML-DSA-44, ML-DSA-65, and ML-DSA-87. The algorithms are added to the `KeyPairGenerator`, `KeyFactory`, and `Signature` rows of the SUN provider table of the JDK Security Providers Guide.

JDK-8333867

Summary: SHA3 performance can be improved

Description: The performance of the `MessageDigest` implementations that belong to the SHA3 family (SHA3-224, SHA3-256, SHA3-384, and SHA3-512) has been improved by 6-27%, depending on digested message length and on the platform used. An additional 30-40% can be experienced on AVX-512 capable platforms due to new intrinsic implementations on that platform.

Issue ID

JDK-8347938

Summary: Add Support for the Latest ML-KEM and ML-DSA Private Key Encodings

Description: The JDK now encodes ML-KEM and ML-DSA private keys in PKCS #8 format using the DER-encoded ASN.1 CHOICE formats defined in [Section 6, 'Private Key Format'](#) of RFC 9935 and [Section 6, 'Private Key Format'](#) of RFC 9881. Two new security properties, `jdk.mlkem.pkcs8.encoding` and `jdk.mldsa.pkcs8.encoding`, control the encoding used when generating new keys with a `KeyPairGenerator` or when translating keys with a `KeyFactory`. Valid values are `seed`, `expandedKey`, and `both` (case-insensitive). If a system property of the same name is also specified, it supersedes the security property value. All three formats are supported when decoding previously encoded private keys with a `KeyFactory`. The default encoding for newly generated ML-KEM and ML-DSA private keys is `seed`. Applications that require a particular private-key encoding can configure the relevant security property or equivalent system property.

JDK-8354305

Summary: SHAKE128 and SHAKE256 MessageDigest algorithms

Description: Two new `MessageDigest` algorithms, SHAKE128-256 and SHAKE256-512, have been added to the SUN provider. These are fixed-length versions of the SHAKE128 and SHAKE256 Extendable-Output Functions (XOFs) defined in NIST FIPS 202. For more information, see [the SUN Provider](#).

JDK-8386991

Summary: Insets are incorrectly set in newer Gnome versions

Description: Insets may change 'in-flight' if the Mutter with `mutter-x11-frames` property (`isTargetUndecorated()` && `isVisible()`) is present. Therefore, The actual values of insets are received from the WM and propagated through all the proper channels.

Issue ID	
JDK-8387123	Summary: Remove LuxTrust Global Root CA Description: The following root certificate has been removed from the <code>cacerts</code> keystore: alias name "luxtrustglobalrootca [jdk]" Distinguished Name: CN=LuxTrust Global Root, O=LuxTrust s.a., C=LU
JDK-8388214	Summary: Update Timezone Data to 2026c Description: Briefly: Alberta moved to permanent -06 on 2026-06-18; Morocco moves to permanent +00 on 2026-09-20; More integer overflow bugs have been fixed in <code>zic</code>.
JDK-8392377	Summary: Update Timezone Data to 2026d Description: Briefly: Canada's Northwest Territories moved to permanent -06 on 2026-08-21; Obsolete settings like <code>TZ='EST5EDT'</code> now conform better to POSIX; Fix security, performance and porting bugs in <code>zic</code> and <code>localtime</code>.
JDK-8392538	Summary: Align the JDK with Microsoft's new timezone names for British Columbia/Alberta Description: Microsoft announced a new timezone name for British Columbia, per https://techcommunity.microsoft.com/blog/dstblog/interim-guidance-for-british-columbia-time-zone-changes-2026/4544988 JDK timezone data needs to be aligned with the registry key updates to allow a Windows user to select a local timezone.
JDK-8393337	Summary: Update Timezone Data to 2026e Description: Briefly: Manitoba moves to permanent -05 on 2026-10-31.

Issue ID

JDK-8393848

Summary: Align the JDK with Microsoft's new timezone name for Manitoba

Description: Microsoft announced a new timezone name for Manitoba, per <https://techcommunity.microsoft.com/blog/dstblog/interim-guidance-for-manitoba-permanent-dst-2026/4562488> JDK timezone data needs to be aligned with the registry key updates to allow a Windows user to select a local timezone.

Builds of Liberica JDK With CRaC

This release of Liberica JDK includes full CRaC support. CRaC support is available for Liberica JDK 17 and 21. For more information, see [Using CRaC with Java applications](#).

IANA TZ Data version

This release of Liberica JDK 17.0.21 comes with the 2026e version of the in-tree copy of the [Time Zone Database](#). The following are the key features of this version.

Briefly

Manitoba moves to permanent -05 on 2026-10-31.

Changes to future timestamps

Manitoba's 2026-03-08 spring forward was its last foreseeable clock change, as it moved to permanent -05 thereafter. Model this with its traditional abbreviation EST. Although the change to permanent -05 legally takes place on 2026-10-31, temporarily model the change to occur on 2026-11-01 at 02:00 for the same reason as other recent temporary hacks. (Caution: see [NOTE FOR 2026b TEMPORARY HACK FOR CLDR AND CANADA](#) below.)

As the change affects both America/Winnipeg and its backward compatibility link, the obsolescent setting `TZ="Canada/Central"` will now use the abbreviation `EST` for affected timestamps, akin to `TZ="Canada/Pacific"` behavior introduced in 2026b.

Another TZDB release may be needed soon if any of the portions of northwestern Ontario historically aligned with America/Winnipeg do not follow. For now, given the short lead time with Manitoba's announcement, assume that they will, to avoid creating new zones that may not be needed if no divergence occurs.

NOTE FOR 2026b TEMPORARY HACK FOR CLDR AND CANADA

This temporary hack works around a Canadian timekeeping bug in Unicode CLDR 48 and earlier. Unfortunately it also causes `zic 2023d` through `2026a`, in the default slim mode, to generate a TZif file that does not conform to Internet RFC 9636 §3.3. The buggy file in turn causes some TZif readers, including `tzcode` itself, to ignore America/Vancouver's 2026-11-01 02:00 transition from PDT (`tm_isdst=1`) to MST (`tm_isdst=0`). Although the buggy file does not cause any known TZif reader to mishandle UT offsets, caution is advised when using `zic 2023d` through `2026a` to compile data from more-recent tz releases. To work around this problem when using these older `zic` versions, use `'zic -b fat'`.

Changes to past timestamps

In 1925 Ireland fell back on 09-20 not 10-04.

Changes to commentary

Discussion on timekeeping practices in northwestern Ontario has been expanded in light of Manitoba's recent announcement. It is not yet known whether or to what extent these areas may adapt their own timekeeping practices in response.

For more information, see [JDK-8393337](#).

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-2026-101516	6.5	security-libs	java.security	network	low	none	none	unchanged	low	low	none
CVE-2026-43660	7.5	javafx	web	network	high	none	required	unchanged	high	high	high
CVE-2026-46470	4.2	javafx	media	network	high	none	required	unchanged	low	none	low
CVE-2026-6732	5.9	javafx	libxml2	network	high	none	none	unchanged	none	none	high
CVE-2026-83374	5.9	security-libs	javax.crypto	network	high	none	none	unchanged	none	high	none
CVE-2026-83376	3.7	security-libs	java.security	network	high	none	none	unchanged	none	low	none
CVE-2026-83380	5.3	security-libs	javax.security	network	low	none	none	unchanged	low	none	none
CVE-2026-83381	4.8	security-libs	javax.security	network	high	none	none	unchanged	low	low	none
CVE-2026-83387	5.9	core-libs	java.sql	network	high	none	none	unchanged	high	none	none
CVE-2026-83395	3.7	core-libs	java.net	network	high	none	none	unchanged	none	low	none
CVE-2026-83400	5.3	xml	jaxp	network	low	none	none	unchanged	none	none	low
CVE-2026-87290	3.7	xml	jaxp	network	high	none	none	unchanged	low	none	none
CVE-2026-87292	3.7	core-libs	java.net	network	high	none	none	unchanged	none	low	none
CVE-2026-87294	6.5	security-libs	java.security	network	low	none	none	unchanged	low	low	none
CVE-2026-87367	3.7	xml	jaxp	network	high	none	none	unchanged	none	low	none
CVE-2026-91332	5.3	core-libs	java.net	network	low	none	none	unchanged	none	low	none
CVE-2026-91334	3.7	client-libs	javax.imageio	network	high	none	none	unchanged	low	none	none
CVE-2026-91335	2.6	client-libs	java.awt	network	high	low	required	unchanged	low	none	none
CVE-2026-91373	5.3	security-libs	java.security	network	low	none	none	unchanged	none	none	low
CVE-2026-91374	4.8	core-svc	tools	network	high	none	none	unchanged	low	low	none
CVE-2026-91375	4.7	tools	jlink	local	high	none	required	unchanged	none	high	none
CVE-2026-91379	4.7	tools	jshell	local	high	none	required	unchanged	none	high	none
CVE-2026-91380	4.0	core-libs	java.util	local	high	none	none	unchanged	low	low	none
CVE-2026-91382	6.5	client-libs	2d	network	high	none	none	unchanged	none	high	low
CVE-2026-91385	5.4	javafx	web	network	low	none	required	unchanged	low	low	none
CVE-2026-91394	5.9	core-libs	java.net	network	high	none	none	unchanged	high	none	none

CVE ID	CVSS score	Component	Module	Attack Vector	Complexity	Privileges	User Interaction	Scope	Confidentiality	Integrity	Availability
CVE-2026-91397	3.6	core-svc	tools	local	high	none	required	unchanged	none	low	low
CVE-2026-91398	6.8	core-libs	java.net	network	high	none	none	changed	none	high	none
CVE-2026-91400	3.1	client-libs	javax.sound	network	high	none	required	unchanged	none	none	low
CVE-2026-91402	3.1	javafx	graphics	network	high	none	required	unchanged	low	none	none
CVE-2026-91410	5.3	core-libs	java.nio	network	low	none	none	unchanged	none	none	low
CVE-2026-91411	6.5	security-libs	org.ietf.jgss	network	high	none	none	unchanged	none	low	high
CVE-2026-91415	4.8	client-libs	2d	network	high	none	none	unchanged	low	low	none
CVE-2026-91418	5.3	client-libs	javax.imageio	network	low	none	none	unchanged	none	none	low
CVE-2026-91451	5.3	core-libs	java.net	network	low	none	none	unchanged	none	low	none
CVE-2026-91452	5.3	core-libs	java.net	network	low	none	none	unchanged	none	low	none
CVE-2026-91453	5.3	core-libs	java.net	network	low	none	none	unchanged	none	low	none
CVE-2026-91461	3.7	security-libs	javax.net.ssl	network	high	none	none	unchanged	none	low	none
CVE-2026-91462	5.9	security-libs	org.ietf.jgss	network	high	none	none	unchanged	none	high	none
CVE-2026-91463	5.3	security-libs	org.ietf.jgss	network	high	none	required	unchanged	high	none	none
CVE-2026-91464	5.3	security-libs	org.ietf.jgss	network	high	none	required	unchanged	high	none	none
CVE-2026-91487	4.8	hotspot	compiler	network	high	none	none	unchanged	low	low	none

5. Resolved Issues

JDK issues

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

Issue ID	Summary
JDK-6626492	Event time in future part 2, now on X
JDK-7067310	3 tests from closed/javax/sound/sampled caused BSOD on win 7 x86
JDK-8023814	Test java/awt/im/memoryleak/InputContextMemoryLeakTest.java fails
JDK-8129778	Few awt test fail for Solaris 11 with RuntimeException
JDK-8148041	Test java/awt/Mouse/TitleBarDoubleClick/TitleBarDoubleClick fails on Ubuntu with mouseReleased event after double click on title bar
JDK-8164464	Consistent failure of java/awt/dnd/MissingEventsOnModalDialog/MissingEventsOnModalDialogTest.java
JDK-8168388	GetMousePositionTest fails with the message "Mouse position should not be null"
JDK-8189441	Define algorithm names for keys derived from KeyAgreement
JDK-8194946	Regression automated Test 'javax/swing/JFileChooser/6738668/bug6738668.java' fails

Issue ID	Summary
JDK-8196018	java/awt/Scrollbar/ScrollbarMouseWheelTest/ScrollbarMouseWheelTest.java fails
JDK-8196367	java/awt/List/SingleModeDeselect/SingleModeDeselect.java times out
JDK-8196440	Regression automated Test 'java/awt/TrayIcon/PopupMenuLeakTest/PopupMenuLeakTest.java' fails
JDK-8202932	java/awt/Component/NativeInLightShow/NativeInLightShow.java fails
JDK-8213120	java/awt/TextArea/AutoScrollOnSelectAndAppend/AutoScrollOnSelectAndAppend.java fails on mac10.13
JDK-8213530	Test java/awt/Modal/ToFront/DialogToFrontModeless1Test.java fails on Linux
JDK-8267617	Certificate's IP x509 NameConstraints raises ArrayIndexOutOfBoundsException
JDK-8270915	GIFImageReader disregards ignoreMetadata flag which causes memory exhaustion
JDK-8275047	Optimize existing fill stubs for AVX-512 target
JDK-8275914	SHA3: changing java implementation to help C2 create high- performance code
JDK-8278102	containers/docker/TestJcmd.java failed with "RuntimeException: Could not find specified process"

Issue ID	Summary
JDK-8279800	isAssignableFrom checks in AlgorithmParametersSpi.engineGetParameterSpec appear to be backwards
JDK-8279954	java/lang/StringBuffer(StringBuilder)/HugeCapacity.java intermittently fails
JDK-8280404	Unexpected exception thrown when CEN file entry comment length is not valid
JDK-8282633	jarsigner output does not explain why an EC key is disabled if its curve has been disabled
JDK-8284813	x86 Code cleanup related to move instructions.
JDK-8284965	closed test sun/java2d/OpenGL/XORPaint.java is unstable
JDK-8286737	Test vmTestbase/gc/gctests/WeakReference/weak006/weak006.java fails: Last soft reference has not been cleared
JDK-8295698	AArch64: test/jdk/sun/security/ec/ed/EdDSATest.java failed with -XX:+UseSHA3Intrinsics
JDK-8296405	java/util/concurrent/forkjoin/AsyncShutdownNow.java is too slow
JDK-8296910	Add EdDSA/XDH/RSASSA-PSS to KeyPairGeneratorBench.java
JDK-8298240	Replace the usage of ImageLayoutException by the CMMException
JDK-8298387	Implement JEP 497: Quantum-Resistant Module-Lattice-Based Digital Signature Algorithm
JDK-8298390	Implement JEP 496: Quantum-Resistant Module-Lattice-Based Key Encapsulation Mechanism

Issue ID	Summary
JDK-8300167	Add validation of the raster's layout before using in native
JDK-8300399	EdDSA does not verify when there is no message
JDK-8300805	Update autoconf build-aux files with latest from 2022-09-17
JDK-8301793	AlgorithmId should not encode a missing parameters field as NULL unless hardcoded
JDK-8303136	MemoryPoolMBean/isCollectionUsageThresholdExceeded/isexceeded005 failed with "isCollectionUsageThresholdExceeded() returned true, while threshold = 1 and used = 0"
JDK-8304013	Add a fast, non-manual alternative to test/jdk/java/util/zip/ZipFile/TestTooManyEntries
JDK-8304701	Request with timeout aborts later in-flight request on HTTP/1.1 cxn
JDK-8305714	Add an extra test for JDK-8292755
JDK-8305780	javax/swing/JTable/7068740/bug7068740.java fails on Ubuntu 20.04
JDK-8307574	ClipIsRunningAfterStop.java failed with <code>"../nptl/pthread_mutex_lock.c:81: pthread_mutex_lock: Assertion `mutex->data.__owner == 0' failed."</code>
JDK-8308395	javax/sound/sampled/Clip/ClipFlushCrash.java timed out
JDK-8308474	DSA does not reset SecureRandom when initSign is called again
JDK-8310331	JitTester: Exclude java.lang.Math.random
JDK-8313612	Use JUnit in lib-test/jdk tests

Issue ID	Summary
JDK-8316391	(zipfs) ZipFileSystem.readFullyAt does not tolerate short reads
JDK-8317126	Redundant entries in Windows tz mappings file
JDK-8318662	Refactor some jdk/java/net/httpclient/http2 tests to JUnit
JDK-8320192	SHAKE256 does not work correctly if $n \geq 137$
JDK-8325506	Ensure randomness is only read from provided SecureRandom object
JDK-8333754	Add a Test against ECDSA and ECDH NIST Test vector
JDK-8333857	Test sun/security/ssl/SSLSessionImpl/ResumeChecksServer.java failed: Existing session was used
JDK-8333867	SHA3 performance can be improved
JDK-8334502	gtest/GTestWrapper.java fails on armhf due to LogDecorations.iso8601_utctime_test
JDK-8338587	Internal XOF Methods for SHAKE128 and SHAKE256
JDK-8340327	A common framework to support public key algorithms with standard parameter sets
JDK-8340493	Fix some Asserts failure messages
JDK-8341625	Improve ZipFile validation of the END header
JDK-8342002	sun/security/tools/keytool/GenKeyPairSigner.java failed due to missing certificate output
JDK-8342003	ProblemList sun/security/tools/keytool/GenKeyPairSigner.java

Issue ID	Summary
JDK-8342442	Static ACVP sample tests
JDK-8343342	java/io/File/GetXSpace.java fails on Windows with CD-ROM drive
JDK-8343739	Test java/awt/event/KeyEvent/ExtendedKeyCode/ExtendedKeyCodeTest. java failed: Wrong extended key code
JDK-8343788	Provide means to alter lib/tzmappings entries on Windows
JDK-8345057	ML_KEM NamedParameterSpec constants removed by ML-DSA integration
JDK-8345512	Remove wrapper functions for intrinsics in PQC algorithms
JDK-8345533	Switch ML-DSA implementation to FIPS 204 final
JDK-8345684	OperatingSystemMXBean.getSystemCpuLoad() throws NPE
JDK-8346683	Problem list automated tests that fail on macOS15
JDK-8347606	Optimize Java implementation of ML-DSA
JDK-8347608	Optimize Java implementation of ML-KEM
JDK-8347938	Add Support for the Latest ML-KEM and ML-DSA Private Key Encodings
JDK-8348309	MultiNST tests need more debugging and timing
JDK-8348561	Add aarch64 intrinsics for ML-DSA
JDK-8349017	Update ML tests to verify against ACVP 1.1.0.38 version

Issue ID	Summary
JDK-8349721	Add aarch64 intrinsics for ML-KEM
JDK-8349759	Add unit test for CertificateBuilder and SimpleOCSPServer test utilities
JDK-8349959	Test CR6740048.java passes unexpectedly missing CR6740048.xsd
JDK-8350589	Investigate cleaner implementation of AArch64 ML-DSA intrinsic introduced in JDK-8348561
JDK-8352149	Test java/awt/Frame/MultiScreenTest.java fails: Window list is empty
JDK-8353478	Update crypto microbenchmarks to cover ML-DSA, ML-KEM, and HSS algorithms
JDK-8354305	SHAKE128 and SHAKE256 MessageDigest algorithms
JDK-8354926	Remove remnants of debugging in the fix for JDK-8348561 and JDK-8349721
JDK-8355241	Move NativeDialogToFrontBackTest.java PL test to manual category
JDK-8356051	Update SignatureUtil.java with the new KnownOIDs
JDK-8356695	java/lang/StringBuilder/HugeCapacity.java failing with OOME
JDK-8359735	[Ubuntu 25.10] java/lang/ProcessBuilder/Basic.java, java/lang/ProcessHandle/InfoTest.java fail due to rust-coreutils
JDK-8360395	sun/security/tools/keytool/i18n.java user country is current user location instead of the language

Issue ID	Summary
JDK-8360562	sun/security/tools/keytool/i18n.java add an ability to add comment for failures
JDK-8361125	Fix typo in onTradAbsence
JDK-8361894	sun/security/krb5/config/native/TestDynamicStore.java ensure that the test is run with sudo
JDK-8365398	TEST_BUG: java/rmi/transport/checkLeaseInfoLeak/CheckLeaseLeak.java failing intermittently
JDK-8365426	[macos26] Graphics2D tests fail on new macOS 26
JDK-8365498	jdk/jfr/event/os/TestCPULoad.java fails with Expected at least one event
JDK-8365776	Convert JShell tests to use JUnit instead of TestNG
JDK-8365861	test/jdk/sun/security/pkcs11/Provider/ tests skipped without SkippedException
JDK-8365863	/test/jdk/sun/security/pkcs11/Cipher tests skip without SkippedException
JDK-8365983	Tests should throw SkippedException when SCTP not supported
JDK-8366182	Some PKCS11Tests are being skipped when they shouldn't
JDK-8367096	jdk/open/test/jdk/sun/security/pkcs11/ rsa, ec, config, secmod and sslecc tests are skipping but showing as pass
JDK-8368677	acvp test should throw SkippedException when no ACVP-Server available

Issue ID	Summary
JDK-8368694	PKCS11-NSS generic keys generated by DH have leading zeroes stripped
JDK-8372546	UnixMultiResolutionSplashTest.java fails intermittently on Ubuntu_24.04
JDK-8372757	MacOS, Accessibility: Crash in [MenuAccessibility accessibilityChildren] after JDK-8341311
JDK-8373632	Some sound tests failing in CI due to lack of sound key
JDK-8373677	Clear text HttpServer connection could fail fast if receiving SSL ClientHello
JDK-8373793	TestDynamicStore.java '/manual' disables use of '/timeout'
JDK-8373796	Refactor java/net/httpclient/ThrowingPublishers*.java tests to use JUnit5
JDK-8373832	Test java/lang/invoke/TestVHInvokerCaching.java tests nothing
JDK-8373866	Refactor java/net/httpclient/ThrowingSubscribers*.java tests to use JUnit5
JDK-8374434	Several JShell tests report JUnit discovery warnings
JDK-8374452	[17u] TestUseSHA512IntrinsicsOptionOnUnsupportedCPU failed with java.lang.AssertionError
JDK-8374755	ML-KEM's 12-bit decompression can be simplified on aarch64
JDK-8374886	CAInterop.java#microsoftrsa2017 test fails as EE certificate does not specify OCSP responder

Issue ID	Summary
JDK-8375125	assert(false) failed: "Attempting to acquire lock NativeHeapTrimmer_lock/nosafepoint out of order with lock ConcurrentHashTableResize_lock/nosafepoint-2 — possible deadlock" when using native heap trimmer
JDK-8376151	Test javax/swing/JFileChooser/4966171/bug4966171.java is failing with OOME
JDK-8377347	jdk/jfr/event/gc/detailed/TestZAllocationStallEvent.java intermittent OOME
JDK-8377983	(zipfs) ZipFileSystem.initCEN needlessly reads END header
JDK-8377991	TestLimitsUpdating.java fails with runtime exception even after JDK-8370492 is fixed
JDK-8377992	(zipfs) Align ZipFileSystem END header validation with the ZipFile implementation
JDK-8378180	Compiling OpenJDK with C23 C-Compiler gives warning: initialization discards 'const' qualifier from pointer target type
JDK-8378506	[macOS] Window content not updated when rendering to multiple windows
JDK-8378878	Refactor java/nio/channels/AsynchronousSocketChannel test to use JUnit
JDK-8379515	draft-ietf-lamps-kyber-certificates is now RFC 9935
JDK-8380011	Path-to-gcroots search should not trigger stack overflows
JDK-8380223	Refactor test/jdk/sun/util/resources TestNG tests to JUnit
JDK-8380715	Enhance PKCS5 padding

Issue ID	Summary
JDK-8380993	[REDO] Incorrect Interpretation of POSIX TZ Environment Variable on AIX
JDK-8381379	Support std/dstOffset attributes in CLDR's metazone definitions
JDK-8381771	Add a check for DNS label not to end with a hyphen
JDK-8381937	Make exceptions in Java_sun_security_mscapi_CKeyPairGenerator generateCKeyPair more specific
JDK-8382178	Enhance TLS certificate handling
JDK-8382407	Enhance LDAP Lookups
JDK-8383047	Enhance LDAP logins
JDK-8383076	Enhance SASL Authentication
JDK-8383281	Enhance MD5 Digesting
JDK-8383301	Enhance WebRowSets
JDK-8383439	Enhance HTTP Client Response Handling
JDK-8383679	Enhance Certificate Name Checks
JDK-8383699	Enhance XPath Expressions
JDK-8383756	Enhance Network Clients
JDK-8384021	Enhance Certificate Constraint Checking
JDK-8384031	Enhance XML Processing

Issue ID	Summary
JDK-8384445	Enhance JPEG loading
JDK-8384455	Enhance DataFlavor
JDK-8384468	Enhance jpackage Packaging
JDK-8384654	Enhance Template Handling
JDK-8384664	Enhance Image Handling
JDK-8384688	Enhance jmod handling
JDK-8384736	Enhance JShell 8387235: JShell tests failing
JDK-8384746	Enhance Preferences
JDK-8384771	Enhance TLS handshakes
JDK-8384872	Enhance HTTP Client
JDK-8384930	Enhance jstatd
JDK-8385209	Enhance HTTP client caching
JDK-8385249	Enhance diagnostic sessions
JDK-8385260	Enhance SOCKS5 support
JDK-8385476	Enhance MIDI file handling
JDK-8385509	Bump update version for OpenJDK: jdk-17.0.21

Issue ID	Summary
JDK-8385584	CAInterop.java#buypassclass3ca fails with Intermediate Root CA not found in the chain
JDK-8386013	Enhance EventListenerList
JDK-8386187	Enhance font rendering
JDK-8386273	Some javax/sound/sampled tests fail on systems with high CPU core number and running with high concurrency
JDK-8386515	Enhance HTTP server parsing
JDK-8386525	Enhance HTTP Server Handler
JDK-8386535	Improve HTTP headers
JDK-8386551	Windows build broken because of MSys2/Make update
JDK-8386552	Enhance GIF loading
JDK-8386776	[17u] Test test/langtools/jdk/jshell/UndefinedClassTest.java fails on JDK 17 with java.lang.ThreadDeath
JDK-8386783	WebRowSet empty elements read value of previous element
JDK-8386923	Enhance TLS Extensions
JDK-8386991	Insets are incorrectly set in newer Gnome versions
JDK-8387075	RemoteHostImpl constructor correction (jstatd)
JDK-8387123	Remove LuxTrust Global Root CA
JDK-8387152	Enhance krb5 tokens

Issue ID	Summary
JDK-8387217	Enhance krb5 client
JDK-8387238	Enhance Kerberos validation
JDK-8387625	Add "dt_socket" to <code>CheckedFeatures.notImplemented</code> for Windows/ARM64
JDK-8388214	(tz) Update Timezone Data to 2026c
JDK-8389492	[21u] <code>java/io/Serializable/records/ProhibitedMethods.java</code> fails after JDK-8307843 backport in othervm mode
JDK-8389648	[TEST_BUG] <code>java/awt/TextField/CaretPositionTest/CaretPositionTest.java</code> fails in OL-9
JDK-8390325	[17u] <code>test/jdk/sun/security/x509/GeneralName/DNSNameTest.java</code> fails to compile in Java 17 after JDK-8381771 backport
JDK-8390327	[17u] <code>test/jdk/java/net/httpclient/lib/jdk/httpclient/test/lib/common/HttpServerAdapters.java</code> fails to compile in Java 17 after JDK-8343855 backport
JDK-8390380	Cherry-pick metazone changes from CLDR to support tzdata2026c for JDK update releases
JDK-8390388	Cherry-pick tz attributes from newer CLDR data for jdk25u and earlier
JDK-8390400	Enhance C2 comparisons
JDK-8391256	<code>TestZoneTextPrinterParser.java</code> assertion fails with expected: <Mountain Standard Time> but was: <Mountain Daylight Time>

Issue ID	Summary
JDK-8391807	Inconsistent TimeZone Names Displayed across JDK release trains
JDK-8392072	Follow-on fix for Improve certification checking
JDK-8392377	(tz) Update Timezone Data to 2026d
JDK-8392519	Cherry-pick metazone changes from CLDR for tzdata2026d, for JDK update release
JDK-8392538	Align the JDK with Microsoft's new timezone names for British Columbia/Alberta
JDK-8393337	(tz) Update Timezone Data to 2026e
JDK-8393344	Cherry-pick metazone changes from CLDR to support tzdata2026e for JDK update releases
JDK-8393848	Align the JDK with Microsoft's new timezone name for Manitoba
JDK-8394265	[21u] Add explicit zone offset test for America/Rainy_River
JDK-8394772	[17u] Update tzmappings.override location after JDK-8343788 backport

JFX issues

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

Issue ID	Summary
JDK-8272808	Update constant collections to use the new immutable collections - leftovers
JDK-8324326	Update ICU4C to 74.2
JDK-8329874	JavaFX debug builds fail on Linux
JDK-8361644	Update ICU4C to 77.1
JDK-8361648	Update Glib to 2.84.3
JDK-8367374	JavaFX debug builds fail on Windows
JDK-8379561	Remove UNICODE related code from GLib
JDK-8380556	Update WebKit to 625.1
JDK-8383209	Improve JavaFX Scripting Support
JDK-8383219	Enhance JavaFX Document Loading
JDK-8383229	Enhance JavaFX Image Loading
JDK-8383252	Enhance JavaFX DnD
JDK-8383322	Enhance JavaFX Clipboard
JDK-8383332	Improve JavaFX Input Methods
JDK-8383333	Improve JavaFX Drag and Drop
JDK-8384522	Update libxml2 to 2.15.3

Issue ID	Summary
JDK-8384809	Update GStreamer to 1.28.3
JDK-8385198	Enhance JavaFX Resource Loading
JDK-8386486	Improve graphics rendering
JDK-8386859	WebView crashes when calling document.startViewTransition()
JDK-8387337	GlassClipboard: Replace deprecated hash_map and hash_set
JDK-8388451	Additional WebKit 625.1 fixes from WebKitGTK 2.52.5
JDK-8388783	Custom String data cannot be read from the clipboard
JDK-8389515	Memory leak in dshowwrapper - decoded buffers delivered by CSink are never unmapped
JDK-8389783	Crash in JavaFX native glass toolkit during Timer shutdown
JDK-8390086	Change JavaFX release version to 17.0.21 in jfx17u
JDK-8390652	Additional WebKit 625.1 fixes from WebKitGTK 2.52.6

6. Updates to Third Party Libraries

This release does not contain any changes in the third party libraries.

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 17.0.21+11

Release Notes

be//soft