Red Hat build of OpenJDK 17

Release notes for Red Hat build of OpenJDK 17.0.9

Last Updated: 2024-05-03

Red Hat build of OpenJDK 17 Release notes for Red Hat build of OpenJDK 17.0.9

Legal Notice

Copyright © 2024 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

The Release notes for Red Hat build of OpenJDK 17.0.9 document provides an overview of new features in Red Hat build of OpenJDK 17 and a list of potential known issues and possible workarounds.

Table of Contents

PREFACE 3

PROVIDING FEEDBACK ON RED HAT BUILD OF OPENJDK DOCUMENTATION 4

MAKING OPEN SOURCE MORE INCLUSIVE 5

CHAPTER 1. SUPPORT POLICY FOR RED HAT BUILD OF OPENJDK 6

CHAPTER 2. DIFFERENCES FROM UPSTREAM OPENJDK 17 7

CHAPTER 3. RED HAT BUILD OF OPENJDK FEATURES 8
3.1. RED HAT BUILD OF OPENJDK ENHANCEMENTS 8
Increased default group size of TLS Diffie-Hellman 8
-XshowSettings:locale output includes tzdata version 8
Certigna root CA certificate added 8
3.2. RED HAT BUILD OF OPENJDK DEPRECATED FEATURES 9
SECOM Trust Systems root CA1 certificate removed 9

CHAPTER 4. ADVISORIES RELATED TO THIS RELEASE 10

PREFACE

Open Java Development Kit (OpenJDK) is a free and open source implementation of the Java Platform, Standard Edition (Java SE). The Red Hat build of OpenJDK is available in three versions: 8u, 11u, and 17u.

Packages for the Red Hat build of OpenJDK are made available on Red Hat Enterprise Linux and Microsoft Windows and shipped as a JDK and JRE in the Red Hat Ecosystem Catalog.

PROVIDING FEEDBACK ON RED HAT BUILD OF OPENJDK DOCUMENTATION

To report an error or to improve our documentation, log in to your Red Hat Jira account and submit an issue. If you do not have a Red Hat Jira account, then you will be prompted to create an account.

Procedure

1. Click the following link to **create a ticket**.
2. Enter a brief description of the issue in the **Summary**.
3. Provide a detailed description of the issue or enhancement in the **Description**. Include a URL to where the issue occurs in the documentation.
4. Clicking **Submit** creates and routes the issue to the appropriate documentation team.

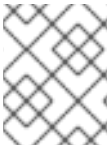
MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

CHAPTER 1. SUPPORT POLICY FOR RED HAT BUILD OF OPENJDK

Red Hat will support select major versions of Red Hat build of OpenJDK in its products. For consistency, these versions remain similar to Oracle JDK versions that are designated as long-term support (LTS).

A major version of Red Hat build of OpenJDK will be supported for a minimum of six years from the time that version is first introduced. For more information, see the OpenJDK Life Cycle and Support Policy .



NOTE

RHEL 6 reached the end of life in November 2020. Because of this, Red Hat build of OpenJDK is not supporting RHEL 6 as a supported configuration..

CHAPTER 2. DIFFERENCES FROM UPSTREAM OPENJDK 17

Red Hat build of OpenJDK in Red Hat Enterprise Linux contains a number of structural changes from the upstream distribution of OpenJDK. The Microsoft Windows version of Red Hat build of OpenJDK attempts to follow Red Hat Enterprise Linux updates as closely as possible.

The following list details the most notable Red Hat build of OpenJDK 17 changes:

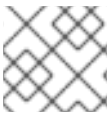
- FIPS support. Red Hat build of OpenJDK 17 automatically detects whether RHEL is in FIPS mode and automatically configures Red Hat build of OpenJDK 17 to operate in that mode. This change does not apply to Red Hat build of OpenJDK builds for Microsoft Windows.
- Cryptographic policy support. Red Hat build of OpenJDK 17 obtains the list of enabled cryptographic algorithms and key size constraints from the RHEL system configuration. These configuration components are used by the Transport Layer Security (TLS) encryption protocol, the certificate path validation, and any signed JARs. You can set different security profiles to balance safety and compatibility. This change does not apply to Red Hat build of OpenJDK builds for Microsoft Windows.
- Red Hat build of OpenJDK on RHEL dynamically links against native libraries such as **zlib** for archive format support and **libjpeg-turbo**, **libpng**, and **giflib** for image support. RHEL also dynamically links against **Harfbuzz** and **Freetype** for font rendering and management. This change does not apply to Red Hat build of OpenJDK builds for Microsoft Windows.
- The **src.zip** file includes the source for all of the JAR libraries shipped with Red Hat build of OpenJDK.
- Red Hat build of OpenJDK on RHEL uses system-wide timezone data files as a source for timezone information.
- Red Hat build of OpenJDK on RHEL uses system-wide CA certificates.
- Red Hat build of OpenJDK on Microsoft Windows includes the latest available timezone data from RHEL.
- Red Hat build of OpenJDK on Microsoft Windows uses the latest available CA certificate from RHEL.

Additional resources

- See, Improve system FIPS detection (RHEL Planning Jira)
- See, Using system-wide cryptographic policies (RHEL documentation)

CHAPTER 3. RED HAT BUILD OF OPENJDK FEATURES

The latest Red Hat build of OpenJDK 17 release might include new features. Additionally, the latest release might enhance, deprecate, or remove features that originated from previous Red Hat build of OpenJDK 17 releases.



NOTE

For all the other changes and security fixes, see OpenJDK 17.0.9 Released.

3.1. RED HAT BUILD OF OPENJDK ENHANCEMENTS

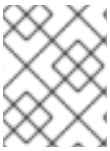
Red Hat build of OpenJDK 17 provides enhancements to features originally created in previous releases of Red Hat build of OpenJDK.

Increased default group size of TLS Diffie-Hellman

In Red Hat build of OpenJDK 17.0.9, the JDK implementation of Transport Layer Security (TLS) 1.2 uses a default Diffie-Hellman key size of 2048 bits. This supersedes the behavior in previous releases where the default Diffie-Hellman key size was 1024 bits.

This enhancement is relevant when a **TLS_DHE** cipher suite is negotiated and either the client or the server does not support Finite Field Diffie-Hellman Ephemeral (FFDHE) parameters. The JDK TLS implementation supports FFDHE, which is enabled by default and can negotiate a stronger key size.

As a workaround, you can revert to the previous key size by setting the **jdk.tls.ephemeralDHKeySize** system property to **1024**. However, to mitigate risk, consider using the default key size of 2048 bits.



NOTE

This change does not affect TLS 1.3, which already uses a minimum Diffie-Hellman key size of 2048 bits.

See JDK-8301700 (JDK Bug System).

-XshowSettings:locale output includes tzdata version

In Red Hat build of OpenJDK 17.0.9, the **-XshowSettings** launcher option also prints the **tzdata** version that the JDK uses. The **tzdata** version is displayed as part of the output for the **-XshowSettings:locale** option.

For example:

```
Locale settings:
    default locale = English
    default display locale = English
    default format locale = English
    tzdata version = 2023c
```

See JDK-8305950 (JDK Bug System).

Certigna root CA certificate added

In Red Hat build of OpenJDK 17.0.9, the **cacerts** truststore includes the Certigna root certificate:

- Name: Certigna (Dhimyotis)

- Alias name: certignarootca
- Distinguished name: CN=Certigna Root CA, OU=0002 48146308100036, O=Dhimyotis, C=FR

See JDK-8314960 (JDK Bug System).

3.2. RED HAT BUILD OF OPENJDK DEPRECATED FEATURES

Review the following release notes to understand pre-existing features that have been either deprecated or removed in Red Hat build of OpenJDK 17.0.9:

SECOM Trust Systems root CA1 certificate removed

Red Hat build of OpenJDK 17.0.9 removes the following root certificate from the **cacerts** truststore:

- Alias name: secomscrootca1 [jdk]
- Distinguished name: OU=Security Communication RootCA1, O=SECOM Trust.net, C=JP

See JDK-8295894 (JDK Bug System).

CHAPTER 4. ADVISORIES RELATED TO THIS RELEASE

The following advisories are issued to document bug fixes and CVE fixes included in this release:

- RHSA-2023:5745
- RHSA-2023:5746
- RHSA-2023:5747
- RHSA-2023:5750
- RHSA-2023:5751
- RHSA-2023:5752
- RHSA-2023:5753

Revised on 2024-05-03 15:37:07 UTC