Red Hat build of OpenJDK 11

Release notes for Red Hat build of OpenJDK 11.0.13

Last Updated: 2024-05-09

Red Hat build of OpenJDK 11 Release notes for Red Hat build of OpenJDK 11.0.13

Legal Notice

Abstract

This document provides an overview of new features in Red Hat build of OpenJDK 11, as well as 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 11 7

CHAPTER 3. RED HAT BUILD OF OPENJDK FEATURES 8
3.1. NEW FEATURES AND ENHANCEMENTS 8
3.1.1. Removed IdenTrust root certificate 8
3.1.2. Updated keytool to create AKID from SKID for issuing certificate as specified by RFC 5280 8
3.1.3. Added ChaCha20 and Poly1305 TLS cipher suites 8
3.1.4. Updated the default enabled cipher suites preference 8

CHAPTER 4. PORTABLE BUILD CHANGES 9
4.1. PORTABLE LINUX BUILDS OF OPENJDK 9
4.2. PORTABLE WINDOWS BUILDS OF OPENJDK 9

CHAPTER 5. 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 two versions, Red Hat build of OpenJDK 8u and Red Hat build of OpenJDK 11u.

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.

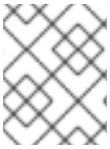
MAKING OPEN SOURCE MORE INCLUSIVE

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 are the same versions that Oracle designates as long-term support (LTS) for the Oracle JDK.

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 11

Red Hat build of OpenJDK in Red Hat Enterprise Linux (RHEL) 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 RHEL updates as closely as possible.

The following list details the most notable Red Hat build of OpenJDK 11 changes:

- FIPS support. Red Hat build of OpenJDK 11 automatically detects whether RHEL is in FIPS mode and automatically configures Red Hat build of OpenJDK 11 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 11 obtains the list of enabled cryptographic algorithms and key size constraints from RHEL. 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.
- The **src.zip** file includes the source for all 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.

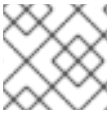
Additional resources

- For more information about detecting if a system is in FIPS mode, see the Improve system FIPS detection example on the Red Hat RHEL Planning Jira.
- For more information about cryptographic policies, see Using system-wide cryptographic policies.

CHAPTER 3. RED HAT BUILD OF OPENJDK FEATURES

3.1. NEW FEATURES AND ENHANCEMENTS

This section describes the new features introduced in this release. It also contains information about changes in the existing features.



NOTE

For all the other changes and security fixes, see OpenJDK 11.0.13 Released.

3.1.1. Removed IdenTrust root certificate

The following root certificate from *IdenTrust* has been removed from the **cacerts** keystore:

- Alias Name: identrustdstx3 [jdk]
- Distinguished Name: CN=DST Root CA X3, O=Digital Signature Trust Co.

For more information, see JDK-8271434.

3.1.2. Updated keytool to create AKID from SKID for issuing certificate as specified by RFC 5280

The **gencert** command of the **keytool** utility has been updated to create AKID from the SKID for issuing certificate as specified by RFC 5280.

For more information, see JDK-8261922.

3.1.3. Added ChaCha20 and Poly1305 TLS cipher suites

The new TLS cipher suites using the **ChaCha20-Poly1305** algorithm are added to JSSE. These cipher suites are enabled by default. The **TLS_CHACHA20_POLY1305_SHA256** cipher suite is available for TLS 1.3.

The following cipher suites are available for TLS 1.2:

- **TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256**
- **TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256**
- **TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256**

For more information, see JDK-8210799.

3.1.4. Updated the default enabled cipher suites preference

The preference of the default enabled cipher suites are changed. The compatibility impact should be minimal. If needed, applications can customize the enabled cipher suites and its preference.

For more information, see JDK-8219551.

CHAPTER 4. PORTABLE BUILD CHANGES

4.1. PORTABLE LINUX BUILDS OF OPENJDK

The portable Linux builds of OpenJDK are available with the FIPS mode. FIPS mode is also available on the RHEL OpenJDK builds. You must install NSS on the portable Linux builds if your system is running in FIPS mode.

4.2. PORTABLE WINDOWS BUILDS OF OPENJDK

The portable Windows builds of OpenJDK are available with the FIPS mode. You do not need to install NSS on the portable Windows builds if your system is running in FIPS mode.

CHAPTER 5. ADVISORIES RELATED TO THIS RELEASE

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

- RHEA-2021:3699-02.
- RHEA-2021:3023-01.
- RHEA-2021:3863-03.

Revised on 2024-05-09 16:46:38 UTC