# Red Hat build of OpenJDK 11

## Release notes for Red Hat build of OpenJDK 11.0.23

Last Updated: 2024-04-17

# Red Hat build of OpenJDK 11 Release notes for Red Hat build of OpenJDK 11.0.23

## Legal Notice



## Abstract

The Release notes for Red Hat build of OpenJDK 11.0.23 document provides an overview of new features in Red Hat build of OpenJDK 11 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 11 ..... 7

CHAPTER 3. RED HAT BUILD OF OPENJDK FEATURES ..... 8

Red Hat build of OpenJDK new features and enhancements 8

XML Signature secure validation mode enabled by default 8

XML Security for Java updated to Apache Santuario 3.0.3 8

SystemTray.isSupported() method returns false on most Linux desktops 9

Certainly R1 and E1 root certificates added 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 four versions: 8u, 11u, 17u, and 21u.

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.

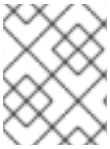
# MAKING OPEN SOURCE MORE INCLUSIVE

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

The latest Red Hat build of OpenJDK 11 release might include new features. Additionally, the latest release might enhance, deprecate, or remove features that originated from previous Red Hat build of OpenJDK 11 releases.

## Red Hat build of OpenJDK new features and enhancements

Review the following release notes to understand new features and feature enhancements that Red Hat build of OpenJDK 11.0.23 provides:

### XML Signature secure validation mode enabled by default

In Red Hat build of OpenJDK 11.0.23, XML Signature secure validation mode is enabled by default. To control restrictions and constraints for secure validation mode, you can use the **jdk.xml.dsig.secureValidationPolicy** system property.

If you want to disable secure validation mode, ensure that the **org.jcp.xml.dsig.secureValidation** property is set to **Boolean.FALSE** by using the **DOMValidateContext.setProperty()** API. Before you disable secure validation mode, ensure that you consider any associated security risks.

See JDK-8259801 (JDK Bug System).

### XML Security for Java updated to Apache Santuario 3.0.3

In Red Hat build of OpenJDK 11.0.23, the XML signature implementation is based on Apache Santuario 3.0.3.

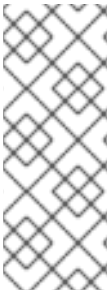
This enhancement introduces the following four SHA-3-based RSA-MGF1 **SignatureMethod** algorithms:

- **SHA3_224_RSA_MGF1**
- **SHA3_256_RSA_MGF1**
- **SHA3_384_RSA_MGF1**
- **SHA3_512_RSA_MGF1**

Because the **javax.xml.crypto.dsig.SignatureMethod** API cannot be modified in update releases to provide constant values for the new algorithms, use the following equivalent string literal values for these algorithms:

- **http://www.w3.org/2007/05/xmldsig-more#sha3-224-rsa-MGF1**
- **http://www.w3.org/2007/05/xmldsig-more#sha3-256-rsa-MGF1**
- **http://www.w3.org/2007/05/xmldsig-more#sha3-384-rsa-MGF1**
- **http://www.w3.org/2007/05/xmldsig-more#sha3-512-rsa-MGF1**

This enhancement also introduces support for the **ED25519** and **ED448** elliptic curve algorithms, which are both Edwards-curve Digital Signature Algorithm (EdDSA) signature schemes.



NOTE

In contrast to the upstream community version of Apache Santuario 3.0.3, the JDK still supports the **here()** function. However, future support for the **here()** function is not guaranteed. You should avoid using **here()** in new XML signatures. You should also update any XML signatures that currently use **here()** to stop using this function. The **here()** function is enabled by default. To disable the **here()** function, ensure that the **jdk.xml.dsig.hereFunctionSupported** system property is set to **false**.

See JDK-8319124 (JDK Bug System).

### SystemTray.isSupported() method returns false on most Linux desktops

In Red Hat build of OpenJDK 11.0.23, the **java.awt.SystemTray.isSupported()** method returns **false** on systems that do not support the **SystemTray** API correctly. This enhancement is in accordance with the **SystemTray** API specification.

The **SystemTray** API is used to interact with the taskbar in the system desktop to provide notifications. **SystemTray** might also include an icon representing an application. Due to an underlying platform issue, GNOME desktop support for taskbar icons has not worked correctly for several years. This platform issue affects the JDK's ability to provide **SystemTray** support on GNOME desktops. This issue typically affects systems that use GNOME Shell 44 or earlier.

NOTE

Because the lack of correct **SystemTray** support is a long-standing issue on some systems, this API enhancement to return **false** on affected systems is likely to have a minimal impact on users.

See JDK-8322750 (JDK Bug System).

### Certainly R1 and E1 root certificates added

In Red Hat build of OpenJDK 11.0.23, the **cacerts** truststore includes two Certainly root certificates:

#### Certificate 1

- Name: Certainly
- Alias name: certainlyrootr1
- Distinguished name: CN=Certainly Root R1, O=Certainly, C=US

#### Certificate 2

- Name: Certainly
- Alias name: certainlyroote1
- Distinguished name: CN=Certainly Root E1, O=Certainly, C=US

See JDK-8321408 (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-2024:1819
- RHSA-2024:1820
- RHSA-2024:1821
- RHSA-2024:1822

*Revised on 2024-04-17 16:12:06 UTC*