



Red Hat build of OpenJDK 11

Release notes for Eclipse Temurin 11.0.21

Legal Notice

Copyright © 2023 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 Eclipse Temurin 11.0.21 provide an overview of new features in OpenJDK 11 and a list of potential known issues and possible workarounds.

Table of Contents

PREFACE	3
MAKING OPEN SOURCE MORE INCLUSIVE	4
CHAPTER 1. SUPPORT POLICY FOR ECLIPSE TEMURIN	5
CHAPTER 2. ECLIPSE TEMURIN FEATURES	6
2.1. NEW FEATURES AND ENHANCEMENTS	6
Increased default group size of TLS Diffie-Hellman	6
Server-side cipher suite preferences used by default	6
Support for RSA keys in PKCS#1 format	6
Output of -XshowSettings:locale option includes tzdata version	6
Certigna root CA certificate added	7
Error thrown if default java.security file fails to load	7
Arrays cloned in several JAAS callback classes	7
2.2. DEPRECATED FEATURES	7
SECOM Trust Systems root CA1 certificate removed	7

PREFACE

Open Java Development Kit (OpenJDK) is a free and open-source implementation of the Java Platform, Standard Edition (Java SE). Eclipse Temurin is available in three LTS versions: OpenJDK 8u, OpenJDK 11u, and OpenJDK 17u.

Binary files for Eclipse Temurin are available for macOS, Microsoft Windows, and multiple Linux x86 Operating Systems including Red Hat Enterprise Linux and Ubuntu.

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 ECLIPSE TEMURIN

Red Hat will support select major versions of Eclipse Temurin 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 Eclipse Temurin will be supported for a minimum of six years from the time that version is first introduced. For more information, see the [Eclipse Temurin Life Cycle and Support Policy](#).



NOTE

RHEL 6 reached the end of life in November 2020. Because of this, Eclipse Temurin does not support RHEL 6 as a supported configuration.

CHAPTER 2. ECLIPSE TEMURIN FEATURES

Eclipse Temurin does not contain structural changes from the upstream distribution of OpenJDK.

For the list of changes and security fixes that the latest OpenJDK 11 release of Eclipse Temurin includes, see [OpenJDK 11.0.21 Released](#).

2.1. NEW FEATURES AND ENHANCEMENTS

Review the following release notes to understand new features and feature enhancements included with the Eclipse Temurin 11.0.21 release:

Increased default group size of TLS Diffie-Hellman

In OpenJDK 11.0.21, the JDK implementation of 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 \(JDK Bug System\)](#).

Server-side cipher suite preferences used by default

In OpenJDK 11.0.21, the SunJSSE provider uses the local server-side cipher suite preferences by default. This supersedes the behavior in previous releases where the server used the preferences that the connecting client specified.

You can revert to the previous behavior by using **SSLParameters.setUseCipherSuitesOrder(false)** on the server side.

See [JDK-8168261 \(JDK Bug System\)](#).

Support for RSA keys in PKCS#1 format

JDK providers can now accept Rivest-Shamir-Adleman (RSA) private and public keys in PKCS#1 format, such as the RSA **KeyFactory.impl** from the SunRsaSign provider. This feature requires that the RSA private or public key object has a PKCS#1 format and an encoding that matches the ASN.1 syntax for a PKCS#1 RSA private key and public key.

See [JDK-8023980 \(JDK Bug System\)](#).

Output of **-XshowSettings:locale** option includes **tzdata** version

In OpenJDK 11.0.21, 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 OpenJDK 11.0.21, the **cacerts** truststore includes the following 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 \(JDK Bug System\)](#).

Error thrown if default **java.security** file fails to load

In previous releases, if the **java.security** file failed to load successfully, OpenJDK used a hardcoded set of security properties. However, this set of properties was poorly maintained and it was not obvious to users that the JDK was using these utilities.

To address this issue, if the **java.security** file fails to load successfully, OpenJDK 11.0.21 throws an **InternalError** instead.

See [JDK-8155246 \(JDK Bug System\)](#).

Arrays cloned in several JAAS callback classes

In previous releases, in the **ChoiceCallback** and **ConfirmationCallback** JAAS classes, when arrays were passed into a constructor or returned, these arrays were not cloned. This behavior allowed an external program to gain access to the internal fields of these classes.

In OpenJDK 11.0.21, the JAAS classes return cloned arrays.

See [JDK-8242330 \(JDK Bug System\)](#).

2.2. DEPRECATED FEATURES

Review the following release notes to understand pre-existing features that have been either deprecated or removed in Eclipse Temurin 11.0.21:

SECOM Trust Systems root CA1 certificate removed

From OpenJDK 11.0.21 onward, the **cacerts** truststore no longer includes the SECOM Trust Systems root certificate:

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

See [JDK-8295894 \(JDK Bug System\)](#).

Revised on 2023-11-02 10:02:00 UTC

