Red Hat build of OpenJDK 17

Release notes for Eclipse Temurin 17.0.8

Last Updated: 2023-11-03

Legal Notice

Abstract

The release notes for Eclipse Temurin 17.0.8 provide an overview of new features in OpenJDK 17 and a list of potential known issues and possible workarounds.

Table of Contents

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.

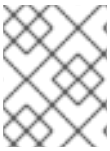
MAKING OPEN SOURCE MORE INCLUSIVE

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 versions remain similar to Oracle JDK versions that Oracle designates as long-term support (LTS).

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 17.0.8.1 RELEASE NOTES

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

Review the following release note for an overview of the changes from the Eclipse Temurin 17.0.8.1 patch release.

NOTE

For all the other changes and security fixes, see OpenJDK 17.0.8.1 Released.

Fixed Invalid CEN header error on valid .zip files

OpenJDK 17.0.8 introduced additional validation checks on the **ZIP64** fields of **.zip** files (JDK-8302483). However, these additional checks caused validation failures on some valid **.zip** files with the following error message: **Invalid CEN header (invalid zip64 extra data field size)**.

To fix this issue, OpenJDK 17.0.8.1 supports zero-length headers and the additional padding that some **ZIP64** creation tools produce. From OpenJDK 17.0.8 onward, you can disable these checks by setting the **jdk.util.zip.disableZip64ExtraFieldValidation** system property to **true**.

See JDK-8313765 (JDK Bug System)

Increased default value of jdk.jar.maxSignatureFileSize system property

OpenJDK 17.0.8 introduced a **jdk.jar.maxSignatureFileSize** system property for configuring the maximum number of bytes that are allowed for the signature-related files in a Java archive (JAR) file (JDK-8300596). By default, the **jdk.jar.maxSignatureFileSize** property was set to 8000000 bytes (8 MB), which was too small for some JAR files.

OpenJDK 17.0.8.1 increases the default value of the **jdk.jar.maxSignatureFileSize** property to 16000000 bytes (16 MB).

See JDK-8313216 (JDK Bug System)

CHAPTER 3. 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 17 release of Eclipse Temurin includes, see OpenJDK 17.0.8 Released.

OpenJDK enhancements

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

Reduced risk of JVM crash when using GregorianCalendar.computeTime()

In OpenJDK 17.0.7, a virtual machine crash could occur when using the **GregorianCalendar.computeTime()** method (JDK-8307683). Even though an old issue is the root cause of this JVM crash, a recent fix for a rare issue in the C2 compiler (JDK-8297951) significantly increased the probability of the JVM crash. To mitigate risk, the OpenJDK 17.0.8 release excludes the fix for the C2 compiler. Once the root cause of the JVM crash is resolved (JDK-8307683), OpenJDK will reintroduce the fix for the C2 compiler (JDK-8297951).

See JDK-8308884 (JDK Bug System).

Support for GB18030-2022

The Chinese Electronics Standardization Institute (CESI) recently published GB18030-2022 as an update to the GB18030 standard, synchronizing the character set with Unicode 11.0. The GB18030-2022 standard is now the default GB18030 character set that OpenJDK 17.0.8 uses. However, this updated character set contains incompatible changes compared with GB18030-2000, which previous releases of OpenJDK 17 used. From OpenJDK 17.0.8 onward, if you want to use the previous version of the character set, ensure that the new system property **jdk.charset.GB18030** is set to **2000**.

See JDK-8301119 (JDK Bug System).

Enhanced ZIP performance

The OpenJDK 17.0.8 release includes enhanced checks on the **ZIP64** fields of **.zip** files. If these checks cause failures on trusted **.zip** files, you can disable these checks by setting the new system property **jdk.util.zip.disableZip64ExtraFieldValidation** to **true**.

JDK bug system reference ID: JDK-8302483.

Enhanced validation of JAR signature

You can now configure the maximum number of bytes that are allowed for the signature-related files in a Java archive (JAR) file by setting a new system property, **jdk.jar.maxSignatureFileSize**. By default, the **jdk.jar.maxSignatureFileSize** property is set to **8000000** bytes (8 MB).

JDK bug system reference ID: JDK-8300596.

GTS root certificate authority (CA) certificates added

In the OpenJDK 17.0.8 release, the **cacerts** truststore includes four Google Trust Services (GTS) root certificates:

Certificate 1

- Name: Google Trust Services LLC
- Alias name: gtsrootcar1
- Distinguished name: CN=GTS Root R1, O=Google Trust Services LLC, C=US

Certificate 2

- Name: Google Trust Services LLC
- Alias name: gtsrootcar2
- Distinguished name: CN=GTS Root R2, O=Google Trust Services LLC, C=US

Certificate 3

- Name: Google Trust Services LLC
- Alias name: gtsrootcar3
- Distinguished name: CN=GTS Root R3, O=Google Trust Services LLC, C=US

Certificate 4

- Name: Google Trust Services LLC
- Alias name: gtsrootcar4
- Distinguished name: CN=GTS Root R4, O=Google Trust Services LLC, C=US

See JDK-8307134 (JDK Bug System).

Microsoft Corporation root CA certificates added

In the OpenJDK 17.0.8 release, the **cacerts** truststore includes two Microsoft Corporation root certificates:

Certificate 1

- Name: Microsoft Corporation
- Alias name: microsoftecc2017
- Distinguished name: CN=Microsoft ECC Root Certificate Authority 2017, O=Microsoft Corporation, C=US

Certificate 2

- Name: Microsoft Corporation
- Alias name: microsoftrsa2017
- Distinguished name: CN=Microsoft RSA Root Certificate Authority 2017, O=Microsoft Corporation, C=US

See JDK-8304760 (JDK Bug System).

TWCA root CA certificate added

In the OpenJDK 17.0.8 release, the **cacerts** truststore includes the Taiwan Certificate Authority (TWCA) root certificate:

- Name: TWCA

- Alias name: twcaglobalrootca
- Distinguished name: CN=TWCA Global Root CA, OU=Root CA, O=TAIWAN-CA, C=TW

See JDK-8305975 (JDK Bug System).

New JFR event jdk.SecurityProviderService

Calls to the **java.security.Provider.getService(String type, String algorithm)** method now trigger a new JFR event, **jdk.SecurityProviderService**.

The **jdk.SecurityProviderService** event contains the following three fields:

- Type: The type of service
- Algorithm: The algorithm name
- Provider: The security provider

The **jdk.SecurityProviderService** event is disabled by default. You can enable this event by using the standard JFR configuration files and options.

See JDK-8254711 (JDK Bug System).

Enhanced contents (trusted certificate entries) of macOS KeychainStore

Recent changes to the macOS **KeychainStore** implementation were incomplete and considered certificates within the user domain only. In the OpenJDK 17.0.8 release, the macOS **KeychainStore** implementation exposes certificates from both the user domain and the administrator domain The macOS **KeychainStore** implementation also now excludes certificates that include a **deny** entry in the trust settings.

See JDK-8303465 (JDK Bug System).

Revised on 2023-11-03 09:35:30 UTC