



Red Hat build of OpenJDK 11

Red Hat build of OpenJDK 11.0.21 发行注记

法律通告

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.

摘要

红帽构建的 OpenJDK 11.0.21 发行注记 文档概述了红帽构建的 OpenJDK 11 中的新功能以及潜在的已知问题列表和可能的临时解决方案。

目录

前言	3
提供有关红帽构建的 OPENJDK 文档的反馈	4
使开源包含更多	5
第 1 章 红帽构建的 OPENJDK 支持政策	6
第 2 章 与上游 OPENJDK 11 的不同	7
第 3 章 RED HAT BUILD OF OPENJDK 功能	8
3.1. 红帽构建的 OPENJDK 新功能及改进	8
3.2. RED HAT BUILD OF OPENJDK 弃用的功能	9
第 4 章 与本发行版本相关的公告	10

前言

Open Java Development Kit (OpenJDK)是 Java Platform, Standard Edition (Java SE)的一个免费的开源实现。红帽构建的 OpenJDK 在三个版本中提供：8u、11u 和 17u。

红帽构建的 OpenJDK 软件包在 Red Hat Enterprise Linux 和 Microsoft Windows 上提供，并作为红帽生态系统目录中的 JDK 和 JRE 提供。

提供有关红帽构建的 OPENJDK 文档的反馈

要报告错误或改进文档，请登录到 Red Hat JIRA 帐户并提交问题。如果您没有 Red Hat Jira 帐户，则会提示您创建一个帐户。

流程

1. 单击以下链接 [以创建 ticket](#)。
2. 在 **Summary** 中输入问题的简短描述。
3. 在 **Description** 中提供问题或功能增强的详细描述。包括一个指向文档中问题的 URL。
4. 点 **Submit** 创建问题，并将问题路由到适当的文档团队。

使开源包含更多

红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看 [CTO Chris Wright 的信息](#)。

第 1 章 红帽构建的 OPENJDK 支持政策

红帽在其产品中支持选择版本的 OpenJDK 的主版本。为实现一致性，这些版本与 Oracle JDK 的长期支持(LTS)指定的版本相同。

自首次引入该版本起，红帽构建的 OpenJDK 主版本将最少提供六年的支持。如需更多信息，请参阅 [OpenJDK 生命周期和支持政策](#)



注意

RHEL 6 于 2020 年 11 月结束其生命周期。因此，红帽构建的 OpenJDK 不支持 RHEL 6 作为支持的配置。

第 2 章 与上游 OPENJDK 11 的不同

Red Hat 在 Red Hat Enterprise Linux (RHEL) 中构建 OpenJDK 包含了来自 OpenJDK 上游发行版的许多结构更改。红帽构建的 Microsoft Windows 版本尝试尽快遵循 RHEL 更新。

以下列表详细介绍了 OpenJDK 11 最显著的红帽构建变化：

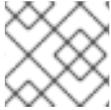
- FIPS 支持。Red Hat build of OpenJDK 11 会自动检测 RHEL 是否处于 FIPS 模式，并自动配置红帽构建的 OpenJDK 11 以在该模式下运行。此更改不适用于适用于 Microsoft Windows 的红帽构建的 OpenJDK 构建。
- 加密策略支持。红帽构建的 OpenJDK 11 从 RHEL 获取启用的加密算法和密钥大小限制列表。这些配置组件由传输层安全(TLS)加密协议、证书路径验证和任何签名的 JAR 使用。您可以设置不同的安全配置集来平衡安全性和兼容性。此更改不适用于适用于 Microsoft Windows 的红帽构建的 OpenJDK 构建。
- RHEL 上的红帽构建的 OpenJDK 会动态链接到原生库，如 **zlib** 用于归档格式支持，**libjpeg-turbo**、**libpng** 和 **giflib** 用于镜像支持。RHEL 还动态链接 **Harfbuzz** 和 **Freetype** 用于字体渲染和管理。
- **src.zip** 文件包含红帽构建的 OpenJDK 附带的所有 JAR 库的源。
- RHEL 上的红帽 OpenJDK 构建使用系统范围的时区数据文件作为时区信息的来源。
- RHEL 上的红帽构建的 OpenJDK 使用系统范围的 CA 证书。
- Microsoft Windows 上的红帽构建的 OpenJDK 包括 RHEL 的最新可用时区数据。
- Microsoft Windows 上的红帽构建的 OpenJDK 使用 RHEL 的最新可用 CA 证书。

其他资源

- 有关检测系统是否处于 FIPS 模式的更多信息，请参阅 Red Hat RHEL 计划 JIRA 中的[增强系统 FIPS 检测示例](#)。
- 有关加密策略的更多信息，请参阅[使用系统范围的加密策略](#)。

第 3 章 RED HAT BUILD OF OPENJDK 功能

最新的 Red Hat build of OpenJDK 11 发行版本可能包括新功能。另外，最新版本可能会增强、弃用或删除来自以前红帽构建的 OpenJDK 11 版本的功能。



注意

有关所有其他更改和安全修复，请参阅 [OpenJDK 11.0.21 发行版本](#)。

3.1. 红帽构建的 OPENJDK 新功能及改进

查看以下发行注记以了解红帽构建的 OpenJDK 11.0.21 提供的新功能和功能改进：

增加 TLS Diffie-Hellman 的默认组大小

在红帽构建的 OpenJDK 11.0.21 中，OpenJDK 实现传输层安全(TLS) 1.2 使用默认的 Diffie-Hellman 密钥大小为 2048 位。这会取代之前版本中的行为，其中默认的 Diffie-Hellman 密钥大小为 1024 位。

当 `TLS_DHE` 密码套件被协商且客户端或服务器不支持 Finite Field Diffie-Hellman Ephemeral (FFDHE) 参数时，这个增强是相关的。JDK TLS 实现支持 FFDHE，它默认是启用的，并可协商更强大的密钥大小。

作为临时解决方案，您可以通过将 `jdk.tls.ephemeralDHKeySize` 系统属性设置为 `1024` 来恢复到以前的密钥大小。但是，为了降低风险，请考虑使用默认密钥 2048 位。



注意

这个更改不会影响 TLS 1.3，它已使用了最小 Diffie-Hellman 密钥 2048 位。

请参阅 [JDK-8301700 \(JDK Bug System\)](#)。

默认使用的服务器端密码套件首选项

在红帽构建的 OpenJDK 11.0.21 中，SunJSSE 供应商默认使用本地服务器端密码套件首选项。这会取代服务器使用连接客户端所指定的首选项的早期版本中的行为。

您可以通过在服务器端使用 `SSLParameters.setUseCipherSuitesOrder (false)` 恢复到之前的行为。

请参阅 [JDK-8168261 \(JDK Bug System\)](#)。

支持 PKCS#1 格式的 RSA 密钥

JDK 供应商现在可以接受 PKCS#1 格式的 Rivest-Shamir-Adleman (RSA) 私钥和公钥，如 `RSA KeyFactory.impl` from the SunRsaSign 供应商。此功能要求 RSA 私钥或公钥对象具有 PKCS#1 格式，以及与 PKCS#1 RSA 私钥和公钥匹配的 ASN.1 语法的编码。

请参阅 [JDK-8023980 \(JDK Bug System\)](#)。

-XshowSettings:locale output 包括 tzdata 版本

在 Red Hat build of OpenJDK 11.0.21 中，`-XshowSettings` launcher 选项还会打印 JDK 使用的 `tzdata` 版本。`tzdata` 版本显示为 `-XshowSettings:locale` 选项的输出的一部分。

例如：

```
Locale settings:
default locale = English
default display locale = English
```

```
default format locale = English
tzdata version = 2023c
```

请参阅 [JDK-8305950 \(JDK Bug System\)](#)。

Certigna root CA 证书

在 Red Hat build of OpenJDK 11.0.21 中，**cacerts** truststore 包括 Certigna root 证书：

- 名称：Certigna (Dhimyotis)
- 别名名称：certignarootca
- 区分名称：CN=Certigna Root CA, OU=0002 48146308100036, O=Dhimyotis, C=FR

请参阅 [JDK-8314960 \(JDK Bug System\)](#)。

如果默认 **java.security** 文件无法加载，则抛出错误

在以前的版本中，如果 **java.security** 文件无法成功加载，Red Hat build of OpenJDK 会使用一组硬编码的安全属性。但是，这组属性不佳维护，JDK 使用这些工具的用户不明显。

要解决这个问题，如果 **java.security** 文件无法成功加载，红帽构建的 OpenJDK 11.0.21 会抛出 **InternalError**。

请参阅 [JDK-8155246 \(JDK Bug System\)](#)。

在几个 JAAS 回调类中克隆的数组

在以前的版本中，当数组传递给构造或返回时，在 **ChoiceCallback** 和 **ConfirmationCallback** JAAS 类中，这些阵列不会被克隆。此行为允许外部程序访问这些类的内部字段。

在红帽构建的 OpenJDK 11.0.21 中，JAAS 类返回克隆的阵列。

请参阅 [JDK-8242330 \(JDK Bug System\)](#)。

3.2. RED HAT BUILD OF OPENJDK 弃用的功能

查看以下发行注记以了解红帽构建的 OpenJDK 11.0.21 中已弃用或删除的预先存在的功能：

SECOM Trust Systems root CA1 证书已删除

从红帽构建的 OpenJDK 11.0.21 开始，**cacerts** truststore 不再包含 SECOM Trust Systems root 证书：

- 别名名称：secomscrootca1 [jdk]
- 可分辨名称：OU=Security communication RootCA1, O=SECOM Trust.net, C=JP

请参阅 [JDK-8295894 \(JDK Bug System\)](#)。

第 4 章 与本发行版本相关的公告

以下公告包括了记录程序错误修复和 CVE 修复：

- [RHSA-2023:5734](#)
- [RHSA-2023:5735](#)
- [RHSA-2023:5736](#)
- [RHSA-2023:5737](#)
- [RHSA-2023:5739](#)
- [RHSA-2023:5740](#)
- [RHSA-2023:5741](#)
- [RHSA-2023:5742](#)
- [RHSA-2023:5743](#)
- [RHSA-2023:5744](#)

更新于 2024-05-10