Red Hat build of OpenJDK 11

Eclipse Temurin 8.0.382 のリリースノート

Last Updated: 2024-05-10

法律上の通知

概要

Eclipse Temurin 8.0.382 のリリースノートには、OpenJDK 8 の新機能の概要と、潜在的な既知の問題と考えられる回避策の一覧が記載されています。

目次

はじめに

Open Java Development Kit (OpenJDK) は、Java Platform Standard Edition (Java SE) のオープンソース実装です。Eclipse Temurin は、OpenJDK 8u、OpenJDK 11u、および OpenJDK 17u の 3 つの LTS バージョンで利用できます。

Eclipse Temurin のバイナリーファイルは、macOS、Microsoft Windows と、Red Hat Enterprise Linux や Ubuntu を含む複数の Linux x86 オペレーティングシステムで利用できます。

RED HAT BUILD OF OPENJDK ドキュメントへのフィードバック

エラーを報告したり、ドキュメントを改善したりするには、Red Hat Jira アカウントにログインし、課題を送信してください。Red Hat Jira アカウントをお持ちでない場合は、アカウントを作成するように求められます。

手順

1. 次のリンクをクリックして **チケットを作成します**。
2. **Summary** に課題の簡単な説明を入力します。
3. **Description** に課題や機能拡張の詳細な説明を入力します。問題があるドキュメントのセクションへの URL を含めてください。
4. **Submit** をクリックすると、課題が作成され、適切なドキュメントチームに転送されます。

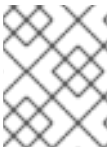
多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージ をご覧ください。

第1章 ECLIPSE TEMURIN のサポートポリシー

Red Hat は、一部の Eclipse Temurin のメジャーバージョンをサポートします。一貫性を保つために、これらのバージョンは、Oracle が Oracle JDK 向けに長期サポート (LTS) を指定しているバージョンと同じになります。

Eclipse Temurin のメジャーバージョンは、バージョンの初回導入時点から最低 6 年間サポートされます。詳細は、Eclipse Temurin Life Cycle and Support Policy を参照してください。



注記

RHEL 6 のライフサイクルは 2020 年 11 月に終了します。このため、Eclipse Temurin はサポート対象の設定として RHEL 6 をサポートしません。

第2章 ECLIPSE TEMURIN の機能

Eclipse Temurin には、OpenJDK のアップストリームディストリビューションの構造の変更は含まれません。

Eclipse Temurin の最新の OpenJDK 11 リリースに含まれる変更点とセキュリティー修正の一覧は、OpenJDK 11.0.20 Released を参照してください。

2.1. 新機能および機能拡張

次のリリースノートを確認して、Eclipse Temurin 8.0.382 リリースに含まれる新機能と機能拡張を理解してください。

TLS Diffie-Hellman のデフォルトのグループサイズが増加しました
OpenJDK 11.0.21 では、TLS 1.2 の JDK 実装はデフォルトの Diffie-Hellman キーサイズ 2048 ビットを使用します。これは、デフォルトの Diffie-Hellman キーサイズが 1024 ビットであった以前のリリースの動作を置き換えるものです。

これは、**TLS_DHE** 暗号スイートがネゴシエートされ、クライアントまたはサーバーのいずれかが Finite Field Diffie-Hellman Ephemeral (FFDHE) パラメーターをサポートしない場合にかかわってくる拡張機能です。JDK TLS 実装は FFDHE をサポートします。FFDHE 、デフォルトで有効になっており、より強力なキーサイズをネゴシエートできます。

回避策として、**jdk.tls.ephemeralDHKeySize** システムプロパティーを **1024** に設定することで、以前のキーサイズに戻すことができます。リスクを軽減するためには、デフォルトのキーサイズである 2048 ビットを使用することを検討してください。

注記

TLS 1.3 はすでに 2048 ビットの最小 Diffie-Hellman キーサイズを使用しているため、この変更の影響は受けません。

JDK-8301700 (JDK Bug System) を参照してください。

サーバー側の暗号スイート設定がデフォルトで使用されるようになりました
OpenJDK 11.0.21 では、SunJSSE プロバイダーはデフォルトでローカルサーバー側の暗号スイートの設定を使用します。これは、サーバーが接続クライアントが指定した設定を使用していた以前のリリースの動作に代わるものです。

サーバー側で **SSLParameters.setUseCipherSuitesOrder(false)** を使用すると、以前の動作に戻すことができます。

JDK-8168261 (JDK Bug System) を参照してください。

PKCS#1 形式の RSA 鍵がサポートされるようになりました
JDK プロバイダーが、SunRsaSign プロバイダーの RSA **KeyFactory.impl** など、PKCS#1 形式の RSA (Rivest-Shamir-Adleman) 秘密鍵および公開鍵を受け入れることができるようになりました。この機能を使用するには、RSA 秘密鍵または公開鍵オブジェクトが PKCS#1 形式であり、PKCS#1 RSA 秘密鍵および公開鍵の ASN.1 構文に一致するエンコーディングである必要があります。

JDK-8023980 (JDK Bug System) を参照してください。

-XshowSettings:locale オプションの出力には、tzdata バージョンが含まれています

OpenJDK 11.0.21 では、**-XshowSettings** launcher オプションは JDK が使用する **tzdata** バージョンも出力します。**tzdata** のバージョンは、**-XshowSettings:locale** オプションの出力の一部として表示されます。

以下に例を示します。

```
Locale settings:
    default locale = English
    default display locale = English
    default format locale = English
    tzdata version = 2023c
```

JDK-8305950 (JDK Bug System) を参照してください。

Certigna ルート CA 証明書の追加

OpenJDK 11.0.21 では、**cacerts** トラストストアに以下の Certigna ルート証明書が含まれています。

- 名前: Certigna (Dhimyotis)
- エイリアス名: certignarootca
- 識別名: CN=Certigna Root CA、OU=0002 48146308100036、O=Dhimyotis、C=FR

JDK-8314960 (JDK Bug System) を参照してください。

デフォルトの java.security ファイルのロードに失敗した場合にエラーが出力されるようになりました

以前のリリースでは、**java.security** ファイルが正常にロードできなかった場合、OpenJDK はハードコーディングされたセキュリティープロパティーのセットを使用していました。しかし、このプロパティーのセットは十分に維持管理されておらず、JDK がこれらのユーティリティーを使用していることがユーザーにはわかりませんでした。

この問題に対処するために、**java.security** ファイルが正常にロードできない場合、OpenJDK 11.0.21 は代わりに **InternalError** を出力します。

JDK-8155246 (JDK バグシステム) を参照してください。

いくつかの JAAS コールバッククラスで配列が複製されるようになりました

以前のリリースでは、**ChoiceCallback** および **ConfirmationCallback** JAAS クラスで、配列がコンストラクターに渡されるとき、または返されるときに、配列が複製されませんでした。この動作により、外部プログラムがこれらのクラスの内部フィールドにアクセスできるようになっていました。

OpenJDK 11.0.21 では、JAAS クラスはクローン作成された配列を返します。

JDK-8242330 (JDK Bug System) を参照してください。

2.2. 非推奨の機能

次のリリースノートを確認して、Eclipse Temurin 11.0.21 で非推奨または削除された既存の機能を理解してください。

SECOM Trust Systems のルート CA1 証明書が削除されました

OpenJDK 11.0.21 以降では、**cacerts** トラストストアに SECOM Trust Systems ルート証明書が含まれなくなりました。

- エイリアス名: secomscrootca1 [jdk]

- 識別名: OU=Security Communication RootCA1、O=SECOM Trust.net、C=JP

JDK-8295894 (JDK Bug System) を参照してください。

改訂日時: 2024-05-10