

Ахіом JDK Pro 8u431+1 Примечания к выпуску

Copyright © 2019-2024 Все права защищены АО "АКСИОМ" (АКСИОМ)

Программное обеспечение АКСИОМ содержит программное обеспечение с открытым исходным кодом. Дополнительная информация о коде сторонних разработчиков доступна на сайте https://axiomjdk.ru/third_party_licenses. Для дополнительной информации о том, как получить копию исходного кода, можно обратиться по адресу info@axiomjdk.ru.

ДАННАЯ ИНФОРМАЦИЯ МОЖЕТ ИЗМЕНЯТЬСЯ БЕЗ ПРЕДВАРИТЕЛЬНОГО УВЕДОМЛЕНИЯ. АКСИОМ ПРЕДОСТАВЛЯЕТ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ "КАК ЕСТЬ" БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, АКСИОМ ПРЯМО ОТКАЗЫВАЕТСЯ ОТ ВСЕХ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ПОДРАЗУМЕВАЕМЫМИ ГАРАНТИЯМИ ТОВАРНОЙ ПРИГОДНОСТИ И ПРИГОДНОСТИ ДЛЯ ОПРЕДЕЛЕННОЙ ЦЕЛИ.

АКСИОМ НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕ НЕСЕТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ КОСВЕННЫЕ, СЛУЧАЙНЫЕ, СПЕЦИАЛЬНЫЕ, ШТРАФНЫЕ ИЛИ КОСВЕННЫЕ УБЫТКИ, ИЛИ УБЫТКИ ОТ ПОТЕРИ ПРИБЫЛИ, ДОХОДА, ДАННЫХ ИЛИ ИСПОЛЬЗОВАНИЯ ДАННЫХ, ПОНЕСЕННЫЕ ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ, БУДЬ ТО В РЕЗУЛЬТАТЕ ДЕЙСТВИЯ ДОГОВОРА ИЛИ ДЕЛИКТА, ДАЖЕ ЕСЛИ АКСИОМ БЫЛО ПРЕДУПРЕЖДЕНО О ВОЗМОЖНОСТИ ТАКИХ УБЫТКОВ.

Использование любого программного продукта АКСИОМ регулируется соответствующим лицензионным соглашением, которое никоим образом не изменяется условиями данного уведомления. Программные продукты и фирменные наименования: Axiom JDK, Axiom JDK Pro, Axiom Runtime Container Pro, Axiom Linux, Libercat, Libercat Certified и АКСИОМ принадлежат АКСИОМ и их использование допускается только с разрешения правообладателя.

Товарный знак Linux® используется в соответствии с сублицензией от Linux Foundation, эксклюзивного лицензиата Линуса Торвальдса, владельца знака на всемирной основе. Java и OpenJDK являются товарными знаками или зарегистрированными товарными знаками компании Oracle и/или ее аффилированных лиц. Другие торговые марки являются собственностью их соответствующих владельцев и используются только в целях идентификации.

Содержание

1. Введение	5
-------------	---

2. Новое в этом выпуске	6
-------------------------	---

Важные исправления	6
--------------------	---

Версия IANA TZData	8
--------------------	---

3. Известные проблемы	9
-----------------------	---

4. Безопасность	10
-----------------	----

5. Дефекты, исправленные в этом выпуске	11
---	----

Исправления в JDK	11
-------------------	----

6. Изменения в сторонних библиотеках	13
--------------------------------------	----

7. Обновление Axiom JDK Pro	14
-----------------------------	----

1. Введение

В этом документе содержится информация о выпуске Axiom JDK Pro 8u431+1.

Axiom JDK Pro является Java SE 8-совместимым дистрибутивом OpenJDK 8, который работает на серверах (Linux x86_64, Linux ARM64, Windows 64), настольных компьютерах (Windows 64, Mac OS x86_64, Mac OS AArch64, Linux x86_64) и встроенных устройствах (Linux ARM64, Linux ARMv7, включая Raspberry Pi 2 & 3 (ARMv6 hardfloat)).

Axiom JDK Pro 8 распространяется в виде файлов `.apk`, `.msi`, `.dmg`, `.deb`, `.rpm`, `.zip` и `.tar.gz`. Пожалуйста, выберите наиболее подходящий вам формат.

2. Новое в этом выпуске

Этот выпуск содержит следующие обновления и новые функции.

Важные исправления

Следующий список содержит важные исправления для версии 8u431.

ID проблемы	
JDK-8330759	<p>Резюме: Отключение набора шифров TLS_ECDH_*</p> <p>Описание: Эти наборы шифров не сохраняют прямую секретность и редко используются на практике. Другие реализации TLS (например, Chrome, Mozilla) не поддерживают эти наборы. В RFC 7525 рекомендуется не использовать эти наборы.</p>
JDK-8332334	<p>Резюме: Добавление двух корневых сертификатов GlobalSign TLS</p> <p>Описание: Корневые сертификаты GlobalSign Root R46 и GlobalSign Root E46 добавлены в хранилище доверенных сертификатов cacerts.</p>
JDK-8336487	<p>Резюме: Смягчение спецификации java.awt.Robot</p> <p>Описание: Это исправление смягчает спецификацию трех методов в классе <code>java.awt.Robot</code> - <code>mouseMove(int, int)</code>, <code>getPixelColor(int, int)</code>, <code>createScreenCapture(Rectangle)</code> и <code>createMultiResolutionScreenCapture(Rectangle)</code> - чтобы разрешить этим методам завершаться сбоем, когда среда рабочего стола не позволяет перемещать указатель мыши или захватывать содержимое экрана.</p>

ID проблемы

JDK-8337230

Резюме: Обновление свойств безопасности и системы JSSE в разделе Customizing JSSE

Описание: Значения по умолчанию для свойств безопасности и системы JSSE в разделе «Настройка JSSE» были обновлены в соответствии со справочным руководством Java Secure Socket Extension (JSSE) Reference Guide: <https://docs.oracle.com/javase/8/docs/technotes/guides/security/jsse/JSSERefGuide.html#InstallationAndCustomization>.

JDK-8339655

Резюме: Отключение поддержки сертификатов сервера TLS, выпущенных после октября 2024 года и привязанных к корневым центрам сертификации Entrust

Описание: Google и Mozilla объявили о планах не доверять сертификатам серверов TLS, выданным Entrust. Это усовершенствование реализует аналогичные ограничения в JDK. Ограничения применяются в SunJSSE, поставщике Java Secure Socket Extension (JSSE) API. Сеанс TLS не будет согласован, если цепочка сертификатов сервера привязана к любому из центров сертификации, указанных здесь, а дата в notBefore указана после 31 октября 2024 года. При необходимости вы можете обойти ограничения, удалив 'ENTRUST_TLS' из свойства безопасности 'jdk.security.caDistrustPolicies'.

JDK-8341125

Резюме: Добавление двух корневых TLS сертификатов SSL.com

Описание: Добавлены новые корневые сертификаты TLS SSL.com, поскольку они будут выпускающим центром сертификации, используемым Entrust.

JDK-8341157

Резюме: Изменение даты окончания действия сертификатов Entrust TLS на 12 ноября 2024 г.

Описание: Google изменила дату 'недоверия' для Entrust с 1 ноября на 12 ноября 2024 года. Entrust также изменила дату, когда они планируют использовать SSL.com в качестве центра сертификации для сертификатов публичных серверов TLS, на 12 ноября. Чтобы соответствовать этим обновленным датам, дата недоверия была изменена на 12 ноября 2024 года.

Версия IANA TZData

Этот выпуск Axiom JDK Pro 8u431 поставляется с версией базы данных часовых поясов IANA [2024a](#). Ниже приведены основные изменения в этом обновлении:

Казахстан объединяется по UTC+5 с 1 марта 2024 г.

Палестина уходит вперед по времени на неделю позже после Рамадана.

``zic`` больше не претендует на поддержку летнего времени на неопределенное время.

``localtime`` теперь правильно обрабатывает Сьюдад-Хуарес в 2422.

3. Известные проблемы

В этой версии отсутствуют известные проблемы.

4. Безопасность

Следующий список содержит исправления уязвимостей для версии 8u431.

CVE ID	CVSS score	Component	Module	Attack Vector	Complexity	Privileges	User Interaction	Scope	Confidentiality	Integrity	Availability
CVE-2023-42950	7.5	javafx	web	network	high	none	required	unchanged	high	high	high
CVE-2024-21208	3.7	core-libs	java.net	network	high	none	none	unchanged	none	none	low
CVE-2024-21210	3.7	hotspot	compiler	network	high	none	none	unchanged	none	low	none
CVE-2024-21217	3.7	core-libs	java.io.serialization	network	high	none	none	unchanged	none	none	low
CVE-2024-21235	4.8	hotspot	compiler	network	high	none	none	unchanged	low	low	none
CVE-2024-25062	7.5	javafx	web	network	low	none	none	unchanged	none	none	high

5. Дефекты, исправленные в этом выпуске

Исправления в JDK

Следующий список содержит дефекты, исправленные в JDK версии 8u431.

ID проблемы	Резюме
JDK-8196770	Add JNDI test com/sun/jndi/ldap/blits/AddTests/AddNewEntry.java
JDK-8233364	Fix undefined behavior in Canonicalizer::do_ShiftOp
JDK-8251188	Update LDAP tests not to use wildcard addresses
JDK-8290367	Update default value and extend the scope of com.sun.jndi.ldap.object.trustSerialData system property
JDK-8313626	C2 crash due to unexpected exception control flow
JDK-8328286	Enhance HTTP client
JDK-8328544	Improve handling of vectorization
JDK-8328726	Better Kerberos support
JDK-8331446	Improve deserialization support
JDK-8332644	Improve graph optimizations

ID проблемы	Резюме
JDK-8335713	Enhance vectorization analysis
JDK-8337664	Distrust TLS server certificates issued after Oct 2024 and anchored by Entrust Root CAs
JDK-8341057	Add 2 SSL.com TLS roots
JDK-8341059	Change Entrust TLS distrust date to November 12, 2024

6. Изменения в сторонних библиотеках

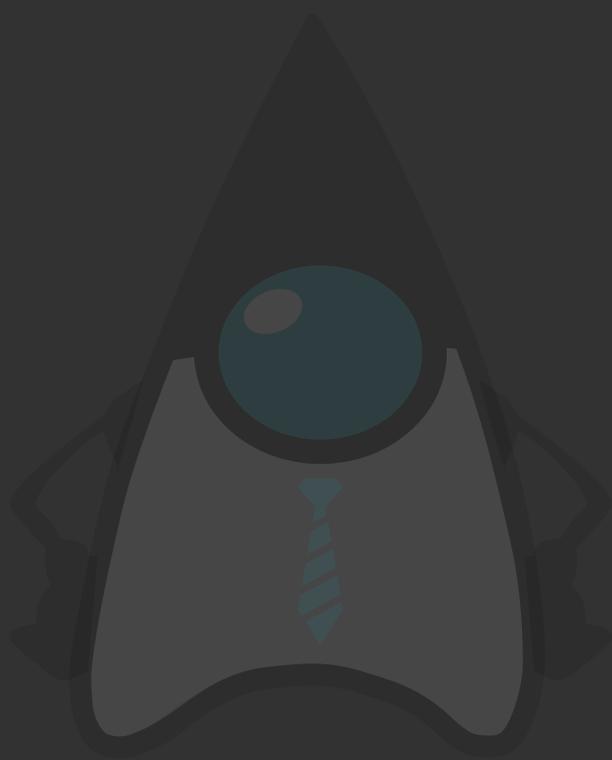
Это список изменений в сторонних библиотеках.

Библиотека	Полное название	Новая версия	Модуль	Номер в системе JBS
zlib	Zlib Data Compression Library	1.3.1	java.base	JDK-8324632

7. Обновление Axiom JDK Pro

Чтобы поддерживать актуальность и безопасность вашего экземпляра Axiom JDK Pro, всегда обновляйтесь до последней доступной версии после ее выпуска. Для обновления установите новую версию поверх предыдущей. Новую версию всегда следует устанавливать и тестировать в непроизводственной среде перед развертыванием в производственной системе.

Инструкции по установке см. в разделе *Установка Axiom JDK* на странице [Axiom JDK](#), либо в разделе документации на [портале поддержки](#). Доступ к этому portalу предоставляется клиентам с активным договором поддержки.



Ахіом JDK Pro 8u431+1
Примечания к выпуску

AXIOM JDK