
Kuali Rice 2.5.9 Release Notes

Released: 05-26-2016

Table of Contents

Overview	1
Release Highlights	1
Download	1
Documentation	1
Contact	2
Items Addressed in Rice 2.5.9	2
Bug Fix	2
New Feature	2
Improvement	2
Impacting Changes	3
Fix XSS vulnerability in returnUrl parameter	3

Overview

Welcome to Rice 2.5.9!

Release Highlights

This release consists of a security fix as well as a number of other bug fixes. The packaged standalone server for this version of Kuali Rice also includes a JAR file for the core-auth-servlet-filter which allows for integration with the CORE authentication service. Additionally, work was done on this release of Kuali Rice to allow for it to be compiled, packaged, and released using a Java 8 compiler. Previous versions supported running on Java 8 but were still being compiled with a Java 7 JDK. Java 7 is still supported in this version of Rice. There are no database changes and this release should be a drop-in replacement.

Download

Kuali Rice 2.5.9 can be downloaded from the Rice website at <http://kuali.org/rice/download>.

There are three different distributions of Rice available: source, binary and server. Please read the [Installation Guide](#) for more details on each of these distributions.

Applications can also consume Rice from the maven site at <http://search.maven.org/#search|ga|1|org.kuali.rice>.

Documentation

API Documentation can be found at <http://site.kuali.org/rice/2.5.9/apidocs/index.html>

Formal documentation can be found at <http://site.kuali.org/rice/2.5.9/reference/html/index.html>. This documentation is still in the process of review and update which will continue through subsequent releases, so please follow the notes in each document to report any outdated information.

Contact

If you encounter any difficulty, please don't hesitate to contact the Rice team on our public collaboration mailing list at <rice.collab@kuali.org>. Please indicate that you are using the 2.5.9 version of Rice.

Items Addressed in Rice 2.5.9

Bug Fix

- [\[KULRICE-14279\]](#) - Fix XSS vulnerability in returnUrl parameter
- [\[KULRICE-14035\]](#) - Issues with document operation screen when trying to open a document that is in EXCEPTION and while deleting branch states
- [\[KULRICE-14280\]](#) - Problem with JPA and wanting to do left outer join on entity bo
- [\[KULRICE-14281\]](#) - Can't inactivate a role delegation on a person - optimistic lock exception
- [\[KULRICE-14283\]](#) - routing and identity management document hierarchy broken
- [\[KULRICE-14284\]](#) - Fix Date (without time) formatting in custom document search result columns
- [\[KULRICE-14285\]](#) - The Active From Date is not retained when adding a role to a Person.
- Fixed issues in UIDocumentService that were causing member-level role responsibility actions in KIM to not save.
- Fixed NPE from calling DocumentRouteHeaderValue.getRoutedByDisplayName where there is no "routed by principal id".
- Fixed an issue where the nested role qualifiers were being converted by the role type of the nested role and not the owning role.
- Fixed various issues that were preventing Rice and it's associated documentation from being packaged and deployed to Maven Central and site.kuali.org using JDK 1.8
- Updated EclipseLinkJpaMetadataProviderImpl, JpaMetadataProviderTest, so that it would properly in the face of different collection order under JDK 1.8
- Added cglib-noddep dependency to KNS module so that it would build properly under JDK 1.8

New Feature

- Added dependency to the "Core" authentication filter (co.kuali:core-filter) in the POM file for the rice-web module. This allows for applications to use Kuali Core for authentication if desired.

Improvement

- Upgraded from 1.0.4-patch8 to 1.0.4-patch9 for OJB
- JDK 1.8 fix - Improved javadoc maven plugin so that it could build Kuali Rice javadocs on JDK 1.8.
- JDK 1.8 fix - Upgraded from ASM 3.3.1 to 5.0.3, this included ensuring the old version of asm was excluded from some dependencies (such as cxf-rt-frontend-jaxws in the KSB client impl module)

- JDK 1.8 fix - Upgraded from Eclipselink 2.5.2 to 2.6.3 due to the following bug: https://bugs.eclipse.org/bugs/show_bug.cgi?id=429992
- JDK 1.8 fix - Updated maven-compiler-plugin configuration to better specify compiling on JDK 1.8 but targeting 1.7 for source and binary compatibility
- JDK 1.8 fix - Switched from `au.com.alderaan:eclipselink-staticweave-maven-plugin` to `de.empulse.eclipselink:staticweave-maven-plugin` for better static bytecode weaving with JDK 1.8

Impacting Changes

Fix XSS vulnerability in returnUrl parameter

This fixes a security issue which has two attack vectors:

- Embedded JavaScript inside of the returnUrl parameter
- Using the returnUrl parameter to return the user to an unexpected domain

The fix to both of these issues involves a new whitelist approach to the values allowed in the returnUrl parameter similar to the whitelist used for pages displayed in the portal. There is a new configuration property named `rice.backLocation.allowed.regex` which controls the URLs which are allowed to be present in the returnUrl parameter. It defaults to a regular expression which would allow URLs which start with the following configuration properties:

- `application.url` (e.g. `my.edu/kfs` or `my.edu/rice` on a standalone Rice server)
- `rice.server.url` (e.g. `my.edu/rice`)
- `appserver.url` (e.g. `my.edu`)

When bringing in this fix you should also ensure the three values above are set appropriately. The third path is intended to be a general "catch all" which would allow any return locations on the same domain as your application. The value for this regular expression may need to be modified if you are using multiple domains for different applications (e.g. `rice.my.edu`, `kfs.my.edu`, etc.), especially on the Rice standalone server since it will need to be configured to allow the user to return to any application which sends the user to the Rice server (e.g. for document search, action list, person lookup, etc.). If the returnUrl does not match one of these paths it will return the user to a configurable location with the `rice.backLocation.default.url` property which defaults to the `application.url`. This value should be customized to return the user to a reasonable location in the case that they attempt to follow an invalid return location.

Bringing in this patch does not guarantee your codebase is immediately secure from this attack. If the `getBackLocation` method on the `KualiForm` or `LookupableHelperService` classes has been overridden in your application you will need to sanitize the return location by invoking the `WebUtils#sanitizeBackLocation` method in order for it to be secure.