Kuali Rice 2.5.6-SNAPSHOT Release Notes

Released: 03-28-2016

Table of Contents

Overview

Welcome to Rice 2.5.6-SNAPSHOT!

Release Highlights

This release consists of a single security fix. There are no database changes and it should be a drop-in replacement.

Download

Kuali Rice 2.5.6-SNAPSHOT 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/2.5.6-SNAPSHOT/apidocs/index.html

Formal documentation can be found at http://site.kuali.org/rice/2.5.6-SNAPSHOT/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and update which will continue through subsequent releases, so please follow the notes in each document to report any outdated information.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 2.5.6-SNAPSHOT version of Rice.

Items Addressed in Rice 2.5.6-SNAPSHOT

Bug Fix

- [KULRICE-14279] - Fix XSS vulnerability in returnLocation parameter

Impacting Changes

Fix XSS vulnerability in returnLocation parameter

This fixes a security issue which has two attack vectors:

- Embedded JavaScript inside of the returnLocation parameter
- Using the returnLocation 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 returnLocation 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 returnLocation 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 returnLocation 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.