

---

# Kuali Rice 2.1.14 Release Notes

Released: 07-22-2016

## Table of Contents

Overview .....	1
Release Highlights .....	1
Download .....	1
Documentation .....	1
Contact .....	1
Impacting Changes .....	2
CSRF Protection for KNS Applications .....	2

## Overview

Welcome to Rice 2.1.14!

## Release Highlights

This release consists of a number of security fixes to the KNS, including the following:

- Cross-Site Request Forgery (CSRF) protection added to the KNS
- Fixed a number of XSS vulnerabilities in the KNS

Depending on your use of the KNS this may be a drop-in replacement. However see below for information on potential impact related to the CSRF implementation.

## Download

Kuali Rice 2.1.14 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/2.1.14/apidocs/index.html>

Formal documentation can be found at <http://site.kuali.org/rice/2.1.14/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and update which will continue through subsequent releases, so please follow the notes in each document to report any outdated information.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](mailto:rice.collab@kuali.org)>. Please indicate that you are using the 2.1.14 version of Rice.

# Impacting Changes

## CSRF Protection for KNS Applications

This release implements CSRF protection within the KNS. For most standard uses of the framework, no action will be required since the fix for this issue has been incorporated into the KNS's `page.tag` library. However, if you are using the KNS with custom JSP pages or HTML and have custom `<form>` elements then you will need to ensure that you are submitting a hidden form input field that contains the CSRF token.

The CSRF token is stored in the session in an attribute called `csrfSessionToken`. There is a new TAG library in the set of KNS tags called "csrf" which will insert the hidden form field and can be used as follows:

```
<kul:csrf />
```

This simply resolves to the following HTML:

```
<input type="hidden" name="csrfToken" value="${sessionScope.csrfSessionToken}" />
```