For end users

Logging in

- To improve security, the handling of the automatic logging in of users has been completely rewritten. Because of this, users will need to log in again with their username and password the first time that they use Jiglu after the upgrade.

Other changes

- If the site has been configured to use external JavaScript, such as analytics, then a banner will now appear asking for permission to accept or reject cookies.
- The use of captchas has been removed. Other mechanisms in the product to prevent abuse were added in version 15 and captchas now offered little additional protection.
- The HTML editor has been upgraded to a new major version. This primarily improves support for newer browsers.
- Line charts with multiple series and pie charts of sources now have improved colours that are also more suitable for those with colour vision deficiency.

Fixes

- Issues with downloading attachments whose filenames contain some Unicode characters have been resolved. Note that UTF-8 surrogate characters are now removed from filenames due to issues in third-party components.
- Spacing issues on some form elements in some browsers have been resolved.
- A small number of other minor issues have been fixed.

For group administrators

Sources

- Passwords for sources are now stored more securely. Because of this change you will need to reset any existing passwords for sources before they can be downloaded again.
- Improvements have been made for handling feeds with whitespace at the beginning of the feed document.

Exporting

- Exported CSV files now include a UTF-8 Byte Order Mark so external programs such as Excel correctly pick up the character set.

For system administrators

User security and passwords

- On the user security system settings category you will find new settings for after how many days a user will be required to log in again and after how many days of not being used an auto-log-in token should be deleted.
- On the user security system settings category there is a new setting for the maximum number of sessions that a user can currently have open on different devices.
- On the user passwords system settings category there is a new setting for the number of iterations to use when encrypting a user's password. This will only affect new passwords after the setting has been changed, in order not to invalidate existing users' passwords.

Cookies

- On the page elements system settings category there is a new setting for the text of the cookie acceptance banner. If this is not empty then users will be prompted for whether to accept or reject cookies the first time that they visit the site.

Logging and admin newsletters

- Activation and deactivation of users by the system will now appear in the system activity log. Previously this would only be shown when carried out by users.
- The administrator newsletter will now list users that were discarded, for example if they did not confirm their email address in time or if an administrator did not accept their request to register in time.

For operations engineers

Upgrade

- Prior to the upgrade, Java 17 must be installed.
- In `bootstrap.properties` there is a new `com.jiglu.external.sourcePasswordEncryptionKey` property which sets the key used to encrypt passwords for sources in the database. This must be added prior to the upgrade together with the new `com.jiglu.external.sourcePasswordIterationCount` property.
- Because of an upgrade to the search system, search indexes will need to be rebuilt. See https://support.jiglu.com/spaces/installation/knowledge/rebuilding-search-indexes for instructions on how to do this if you host your own system.

Other changes

- We have replaced the mechanism by which Jiglu is started and stopped from Linux. Jiglu is also now a `systemd` service rather than using legacy init scripts.
- Jiglu now requires Java 17.
- Third-party libraries have all been updated to their latest recommended versions.

Security

- Two security issues in the processing of SVG files have been resolved, which could potentially have allowed disclosure of internal information (CVE-2022-44730, CVE-2022-44729). This was also resolved in 15.3.2.
- Several cross-site scripting vulnerabilities in the HTML editor have been resolved.
- Improvements to the processing of image metadata have improved robustness and hardened security.