For end users

- Previously if you set up an alert containing certain characters then choosing that alert on the Radar would cause a JavaScript error and a broken page. There were also some related issues with trending tags. These have all been resolved.

- If you try and join a group that you no longer have permission to join then you will now be given a specific error message rather than taken to a general error page.

- Some bad URLs for polls in a space that uses discussion areas have been corrected.

- If you voted in a poll from the Radar then although your vote would be accepted you would also be given a message that the page requested could not be found. This has now been resolved.

- Deleting a tag that is an event type could sometimes fail with a database error. This has been resolved.

- If you uploaded an attachment and there was a problem analysing its content then this would sometimes result in its media type being wrongly corrected. This has been resolved.

- When you included a link in a contribution, sometimes the title or other details for the link would contain visible HTML entity names. This has been resolved.

- There are now limits on what characters may be included in users' given and family names.

- A number of minor issues have been fixed.

For group administrators

- When viewing a discussion thread with a poll, the *Close poll* button now only appears beneath the message that contains the poll.

- Adding a text section to a group home page but not including any text for it could previously result in bad HTML for the page. This has been resolved.

- Member notifications that allow a name placeholder now also have a placeholder just for the user's given name.

- When editing a source, changing the article page pattern will now immediately remove any items that no longer match the pattern and new downloads will be requested for any URLs that the system knows about that match the new pattern.

- A number of issues have been fixed with the source add and edit pages where fields were not being correctly disabled or enabled as options were selected or their values were being lost when certain options were selected.

- Previously when a source was requested to be spidered again this ignored updates even when content extraction selectors had been changed. All pages are now downloaded again when respidering is requested.

For system administrators

Notifications

- User notifications that allow a name placeholder now also have a placeholder just for the user's given name.

Security

- There is a new system setting available in the *Content lookup* category, *Connection blacklist*, which can be used to blacklist IP address ranges to which feeds, spiders and lookups of page metadata cannot be made. This prevents abuse of these features to attack local systems. By default this is set to the private address ranges and the local loopback range. Additionally, links will now only have metadata for them looked up if they use the default http: or https: ports.

- A potential path for remote code execution in the web application has been removed, although this was not exploitable in any recent major or minor versions of the product.

- The Message-ID: for an email originating on the system now uses the mail domain of the system rather than the local host name of the server it is running on.

- When carrying out a search in an LDAP server as part of the process of registering new users, LDAP special characters were not being escaped, which could result in wider searches than allowed or system errors. This has been resolved.

- Two script injection vulnerabilities in group newsletters and vulnerabilities for URLs included in contributions or profiles have been resolved. Significant enhancements to our test suite have been made to safeguard against future XSS vulnerabilities slipping through.

- An external source code security review has resulted in a number of changes to the Jiglu server and web application internals to better protect the system.

System

- If you start the server and the licence key has expired then it will now fall back to the default licence key instead of using the existing key with all modules disabled.

- The PostgreSQL database driver has been updated and now contains a number of new options for connecting to a database over SSL. This change also required the replacement of interfacing code for dealing with the storage of binary data, such as attachments.

- If there is a problem connecting to the database when the server is first started then it will now exit immediately without additional spurious error messages being displayed.

- The memory overhead when the server is working with attachments has been significantly lowered while performance with smaller attachments has been improved.

- Third party libraries have all been updated to the latest recommended versions.