For end users

- You can no longer upload attachments whose filenames contain characters that are not permitted in Windows. If you email a discussion message with an attachment that has such a filename to a group then the invalid characters will be replaced by dashes.
- If you upload an attachment with the wrong extension for its media type the system automatically corrects the media type and the filename. However, the URL for the attachment was previously not being corrected. This has now been resolved.
- Text from form fields is now subject to additional cleaning, including the removal of control characters and duplicate spaces.
- Form fields for users' given and family names are now subject to additional validation.
- An issue that could cause groups to be listed twice in indexes when they required approval before activation has been resolved.
- A small number of minor issues have been fixed.

For group administrators

Tasks

- When a group task is actioned the choice that was taken is now recorded in the activity log with a new event type of 'Task action'.
- In the activity log there are new event types for 'Revise' (when a revision has been requested of a contribution) and 'Schedule' (when a blog post or poll has been scheduled).

For system administrators

Tasks

- When a system task is actioned the choice that was taken is now recorded in the activity log with a new event type of 'Task action'.
- In the activity log there is a new event type for 'Email address change rejected' when an administrator has rejected a request by a user to change their email address.

Security

- There is a new system setting available in the Appearance category controlling whether inline scripts are allowed. This defaults to 'No' but will be needed if you want to use custom JavaScript or users have browsers or firewalls with issues using JSON script blocks or incorrectly block some features when it is not allowed.

- If the system has been configured to permit uploads of XML files, then any XML file must now be downloaded for it to be able to be viewed – it is no longer possible to directly show an XML file in the browser. This prevents a script injection vulnerability using JavaScript in an XML file.

- A number of script injection (XSS) vulnerabilities have been resolved throughout the interface. The scope for injection would have been limited by the size of the fields and the Content Security Policy preventing external script execution. These fixes include:

    - Vulnerabilities in the instant message functionality where user-supplied information was not being escaped when sent over the Talk section web socket.

    - Vulnerabilities in newsletters and enhanced discussion message emails, which were not escaping quote characters for message and attachment tooltip descriptions. While JavaScript would not be executed for HTML email, these would still be vulnerable in the group newsletter previews.

- When plain text input is converted into enhanced HTML (e.g. for plain text discussion messages or instant messages), javascript: protocol links are no longer converted. These would have required a user to click on them and it was not possible to obfuscate them so they would have been clear to users. Additionally, such URLs would have spurious additional spaces added to the text, which has also been resolved.

- The Content Security Policy sent by the system has been tightened. When external content whitelisting is enabled in the Content Filtering system settings page it now sets the allowed URLs for images, frames, media and objects according to what embedded sites are configured and activated rather than allowing them from anywhere.

- You can no longer create a group with an identifier of 'administrator', 'hostmaster', 'root' or 'webmaster'. This prevents a user with group add permission from hijacking these sensitive email addresses.

System

- If a system error occurs in the web app then an identifier will now be shown that allows the error to be more easily located in the web container's logs.

- An issue has been resolved that caused the sendmail milter to fail when imposing a limit on the amount of email allowed from each sender address.

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