Forums | Mahara Community

Cross-site scripting and escalation of privileges in Mahara before 25.04.2 and 24.04.11

This topic is closed. Only moderators and the group administrators can post new replies.

Robert Lyon
Posts: 806

06 October 2025, 15:20

Hello,

This latest release contains two security fixes that are of high importance, depending on the functionality you have enabled on your site. We would like to thank the people who made responsible disclosures of these security issues to us.

A list of fixes is available on the 'Releases' page, accessible to subscribers. We provide fixes for Mahara 24.04 and Mahara 25.04.

This is the last security release for Mahara 24.04. We recommend you upgrade to Mahara 25.04 to continue receiving security updates. Alternatively, you can purchase the Extended Security Support.

Access updates

Subscribers have two options for accessing the latest code.

Via Git

- 25.04 Git branch
- 24.04 Git branch

As downloadable package

The changes are also available on the 'Releases' page as downloadable packages **under the heading 'Mahara download files...'** in each respective release, which also includes a list of issues linked to their descriptions that have been fixed:

- 25.04.2
- 24.04.11

If you use the download files, make sure not to download a file called 'source code'. You want to download the files that have the compiled code as only that will come with all necessary libraries and stylesheet information.

Update information

Please see the wiki for information on updating Mahara, based on the method you use, either via the code repository (Git) or the downloadable package.

CVE information

CVE-2025-59308

Impact: Escalation of privileges

Attack type: Remote

Attack vector: Someone must have the 'Site staff' permission and either 'Institution administrator' or 'Institution support administrator' permissions in one but not other institutions.

Description: In Mahara before version 24.04.10 and before version 25.04.1, an institution administrator or institution support administrator on a multi-tenanted site can masquerade as an institution member in an institution for which they are not an administrator if they also have the 'Site staff' role.

Credit: Kristina Hoeppner (Catalyst IT)
Issue report

CVE-2025-61872

Vulnerability type: Cross-site scripting (XSS)
Attack type: Remote
Impact: Code execution

Affected components: The 'search site' feature when using the Elasticsearch7 search plugin.

Suggested description: Mahara before 25.04.2 and 24.04.11 are vulnerable to displaying results that can cause code execution from a malicious search query string.

Reported by: SinMaven
Issue report

As subscriber, we recommend you update your instance of Mahara to the latest maintenance release of the series of Mahara you are using, or if you are on an unsupported version of Mahara, upgrade to a supported one.

Thank you

The Mahara team at Catalyst

Edits to this post:
 Kristina Hoeppner - Yesterday, 12:54
 Kristina Hoeppner - Yesterday, 13:03

1 result