Forums | Mahara Community

Information disclosure in Mahara before 21.04.6, 21.10.4, and 22.04.2 and all versions of 20.04 and 20.10

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

16 June 2022, 15:48

Kristina Hoeppner
Posts: 4480

Critical

We recommend you install this security update on your site as quickly as possible.

Vulnerability type: Incorrect access control
Attack type: Remote
Impact: Information disclosure

Unsupported versions of Mahara 20.04 and 20.10, and support versions of Mahara 21.04 before 21.04.6, 21.10 before 21.10.4, and 22.04.2 are vulnerable to files being served by thumb.php without a permission check under certain conditions.

Reported by Gwenole T.
Bug report
CVE reference: CVE 2022-33913

Which versions of Mahara are fixed?

Mahara 21.04, 21.10, and 22.04 are currently supported for security fixes. You can download the latest minor point versions 21.04.6, 21.10.4, and 22.04.2 respectively to receive the fix for this security issue.

Mahara 20.04 and 20.10 are not supported with security fixes any more. However, you can patch your site by backporting the fix to your instance, i.e. download the two changed files (or download a patch file) and merge them into your codebase. You may have to resolve merge conflicts, esp. if you changed anything in these files yourself.

Where can I find the security releases?

You can download the latest versions from Launchpad or check out the relevant branch from Git.

Edits to this post:
Kristina Hoeppner - 20 June 2022, 8:45

1 result