

Components:

Description:

This advisory addresses two critical security vulnerabilities present in Mautic versions before 5.2.3. These vulnerabilities could be exploited by authenticated users. * Remote Code Execution (RCE) via Asset Upload: A Remote Code Execution vulnerability has been identified in the asset upload functionality. Insufficient enforcement of allowed file extensions allows an attacker to bypass restrictions and upload executable files, such as PHP scripts. * Path Traversal File Deletion: A Path Traversal vulnerability exists in the upload validation process. Due to improper handling of path components, an authenticated user can manipulate the file deletion process to delete arbitrary files on the host system.

Main problems:

94 "Improper Control of Generation of Code ('Code Injection')"