CVE-2025-1028 - Score: 8.1

Components:

Description:

The Contact Manager plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the contact form upload feature in all versions up to, and including, 8.6.4. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible in specific configurations where the first extension is processed over the final. This vulnerability also requires successfully exploiting a race condition in order to exploit.

Main problems:

434 "Unrestricted Upload of File with Dangerous Type"