CVE-2024-13409 - Score: 7.5

Components:

wpwax post grid\, slider \& carousel ultimate *

Description:

The Post Grid, Slider & Carousel Ultimate with Shortcode, Gutenberg Block & Elementor Widget plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.6.10 via the 'theme' parameter of the post_type_ajax_handler() function. This makes it possible for authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other safe file types can be uploaded and included.

Main problems:

22 "Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')"