

## Description:

The Migration, Backup, Staging WPvivid Backup & Migration plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'upload\\_files' function in all versions up to, and including, 0.9.112. This makes it possible for authenticated attackers, with Administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. NOTE: Uploaded files are only accessible on WordPress instances running on the NGINX web server as the existing .htaccess within the target file upload folder prevents access on Apache servers

## Main problems:

434 "Unrestricted Upload of File with Dangerous Type"