NVD DB Update

CVE-2022-2431 - Score: 8.1

Components:

w3eden download manager *

Description:

The Download Manager plugin for WordPress is vulnerable to arbitrary file deletion in versions up to, and including 3.2.50. This is due to insufficient file type and path validation on the deleteFiles() function found in the ~/Admin/Menu/Packages.php file that triggers upon download post deletion. This makes it possible for contributor level users and above to supply an arbitrary file path via the 'file[files]' parameter when creating a download post and once the user deletes the post the supplied arbitrary file will be deleted. This can be used by attackers to delete the /wp-config.php file which will reset the installation and make it possible for an attacker to achieve remote code execution on the server.

Main problems:

73 "External Control of File Name or Path"