NVD DB Update

CVE-2022-25277 - Score: 7.2

Components:

drupal drupal *

Description:

Drupal core sanitizes filenames with dangerous extensions upon upload (reference: SA-CORE-2020-012) and strips leading and trailing dots from filenames to prevent uploading server configuration files (reference: SA-CORE-2019-010). However, the protections for these two vulnerabilities previously did not work correctly together. As a result, if the site were configured to allow the upload of files with an htaccess extension, these files' filenames would not be properly sanitized. This could allow bypassing the protections provided by Drupal core's default .htaccess files and possible remote code execution on Apache web servers. This issue is mitigated by the fact that it requires a field administrator to explicitly configure a file field to allow htaccess as an extension (a restricted permission), or a contributed module or custom code that overrides allowed file uploads.

Main problems:

434 "Unrestricted Upload of File with Dangerous Type"