givanz / **Vvveb** Public

Code Issues 140 Pull requests 10 Discussions Actions Security an

Commit `6fb8eaa`

givanz committed 3 weeks ago

```
Fixed rename failing to prevent rename to restricted file extension in media
library, 'Remote Code Execution via Chained Rename Bypass and .htaccess PHP
Handler Injection', reported by @kdalal-vulncheck #419
```

`master` · 1.0.8.2 1.0.8.1

1 parent 23ac0e8 commit 6fb8eaa

1 file changed +5 -3

Top

Filter files…

system/traits

media.php

Search within code

system/traits/media.php

```
@@ -205,6 +205,8 @@ function rename() {
205 205         $duplicate   =  $this->request->post['duplicate'] ?? false;
206 206         $dirMedia    = $this->dirMedia;
207 207
    208 +       $this->response->setType('json');
    209 +
208 210         $currentFile = $dirMedia . DS . $file;
209 211         if ($newfile) {
210 212             $targetFile  = $dirMedia . DS . $newfile;
@@ -217,8 +219,9 @@ function rename() {
```

```
217  219            $extension = strtolower(substr($targetFile, strrpos($targetFile, '.') +
                  1));
218  220
219  221            if (isset($this->uploadDenyExtensions) && in_array($extension, $this-
                  >uploadDenyExtensions)) {
220       -            $message .= __('File type not allowed!');
221       -            $success = false;
     222  +            $message = ['success' => false, 'message' => __('File type not
                  allowed!')];
     223  +            $this->response->output($message);
     224  +            return;
222  225            }
223  226
224  227            if ($duplicate) {
          @@ -235,7 +238,6 @@ function rename() {
235  238                }
236  239            }
237  240
238       -            $this->response->setType('json');
239  241            $this->response->output($message);
240  242        }
241  243
```

Comments 0

Please sign in to comment.