WWBN / AVideo Public

Code Issues 13 Pull requests Actions Projects Wiki Security a

Commit bd11c16

Daniel Neto committed last week · 11 / 11

fix: Enhance path traversal protection in URL handling and file access

GHSA-m63r-m9jh-3vc6

master

1 parent bcba324 commit bd11c16

2 files changed +20 -5 lines changed

Top

Filter files...

objects

aVideoEncoderReceiveImage.json.php

functionsFile.php

2 files changed +20 -5 lines changed

Search within code

objects/aVideoEncoderReceiveImage.json.php

```
@@ -43,11 +43,14 @@
43 43
44 44    foreach ($securityChecks as $key => $value) {
45 45        if (!empty($_REQUEST[$value])) {
46    -         // Block directory traversal in URL paths.
47    -         // str_replace('../','') is bypassable via '..../'; instead reject any URL
48    -         // whose decoded path contains '..' (covers '../', '..../'-bypass, and %2e%2e variants).
49    -         $decodedPath = urldecode((string)(parse_url($_REQUEST[$value], PHP_URL_PATH) ?? ''));
50    -         if (strpos($decodedPath, '..') !== false) {
```

```
      46  +         // Block directory traversal in URL paths AND query strings.
      47  +         // The previous check only inspected parse_url(..., PHP_URL_PATH), so a payload
      48  +         // like http://host/x?a=/videos/../../etc/passwd bypassed it entirely because
      49  +         // the '..' appears only in the query string component, not the path.
      50  +         // Decode the full URL string (handles %2e%2e and similar encodings) and reject
      51  +         // any URL that contains '..' anywhere.
      52  +         $decodedFull = urldecode((string)$_REQUEST[$value]);
      53  +         if (strpos($decodedFull, '..') !== false) {
51    54              unset($_REQUEST[$value]);
52    55          }
53    56      }
```

objects/functionsFile.php

```
      @@ -227,6 +227,18 @@ function try_get_contents_from_local($url)
227   227               $encoder = 'Encoder/';
228   228           }
229   229           $tryFile = "{$global['systemRootPath']}{$encoder}videos/{$parts[1]}";
      230 +         // Defense-in-depth: validate the resolved path stays within the videos directory.
      231 +         // explode('/videos/', $url) operates on the full URL string including query string,
      232 +         // so a traversal payload in the query string (e.g. ?a=/videos/../../etc/passwd)
      233 +         // populates $parts[1] with '../../etc/passwd' and escapes the directory.
      234 +         $videosBaseDir = realpath("{$global['systemRootPath']}{$encoder}videos");
      235 +         $realTryFile   = realpath($tryFile);
      236 +         if ($videosBaseDir === false || $realTryFile === false
      237 +             || strpos($realTryFile, $videosBaseDir . DIRECTORY_SEPARATOR) !== 0
      238 +         ) {
      239 +             _error_log("try_get_contents_from_local: blocked path traversal attempt for url={$url}");
      240 +             return false;
      241 +         }
230   242           //_error_log("try_get_contents_from_local {$url} => {$tryFile}");
```

```
231  243            if (file_exists($tryFile)) {
232  244                return file_get_contents($tryFile);
```

Comments 0

Please sign in to comment.