chamilo / **chamilo-lms** Public

Code | Issues 399 | Pull requests 13 | Discussions | Actions | Projects

Commit de4058d

AngelFQC committed 3 weeks ago Verified

```
Security: Refactor URL validation logic to ensure stricter checks against
private/reserved ranges.

See advisory GHSA-g2xj-4cch-j276
```

master · v2.0.0 v2.0.0-RC.3

1 parent f10245a commit de4058d

1 file changed +3 -37 lines changed

Top

Filter files…

public/plugin/Pens/lib

PensProcessor.php

1 file changed +3 -37 lines changed

Search within code

public/plugin/Pens/lib/PensProcessor.php

```
@@ -122,7 +122,7 @@ private function collectPackage(PENSRequestCollect
$request): string
122 122             throw new PENSException(1322);
123 123         }
124 124
125     -       if (!$this->isAllowedDownloadUrl($request->getPackageUrl())) {
    125 +       if (!$this->isAllowedPackageUrl($request->getPackageUrl())) {
126 126             error_log('[Pens][collectPackage] download url rejected');
127 127             throw new PENSException(1301);
128 128         }
@@ -428,26 +428,11 @@ private function isAllowedPackageUrl(string $url):
bool
```

```
428  428         }
429  429
430  430         /**
431       -      * Allow callback URLs pointing to public hosts or to the current Chamilo host.
     431  +      * Allow callback URLs pointing to public hosts only (no private/reserved ranges).
432  432         */
433  433         private function isAllowedCallbackUrl(string $url): bool
434  434         {
435       -         $parts = parse_url($url);
436       -         if (!is_array($parts)) {
437       -             return false;
438       -         }
439       -
440       -         $scheme = strtolower((string) ($parts['scheme'] ?? ''));
441       -         if (!in_array($scheme, ['http', 'https'], true)) {
442       -             return false;
443       -         }
444       -
445       -         $host = strtolower((string) ($parts['host'] ?? ''));
446       -         if ('' === $host) {
447       -             return false;
448       -         }
449       -
450       -         return true;
     435  +         return $this->isAllowedRemoteUrl($url, false);
451  436         }
452  437
453  438         /**
     ↓ ↑   @@ -529,23 +514,4 @@ private function hasZipSignature(string $path): bool
529  514             return in_array($signature, ["PK\x03\x04", "PK\x05\x06", "PK\x07\x08"], true);
530  515         }
531  516
532       -     private function isAllowedDownloadUrl(string $url): bool
533       -     {
534       -         $parts = parse_url($url);
535       -         if (!is_array($parts)) {
```

```
536         -             return false;
537         -         }
538         -
539         -         $scheme = strtolower((string) ($parts['scheme'] ?? ''));
540         -         if (!in_array($scheme, ['http', 'https'], true)) {
541         -             return false;
542         -         }
543         -
544         -         $host = strtolower((string) ($parts['host'] ?? ''));
545         -         if ('' === $host) {
546         -             return false;
547         -         }
548         -
549         -         return true;
550         -     }
551   517     }
```

Comments 0

Please sign in to comment.