Code Analysis

Created Fri 4th Apr 2025 | Snapshot for commit f467fd2 taken by snyk.io 21 hours ago | Retest now

IMPORTED BY
Annam Raghu Pavan

PROJECT OWNER
Add a project owner

ENVIRONMENT
Add a value

BUSINESS CRITICALITY
Add a value

LIFECYCLE
Add a value

ANALYSIS SUMMARY
454 analyzed files (79%) Repo breakdown

Issues 8

Search...

SEVERITY
- High 1
- Medium 0
- Low 7

PRIORITY SCORE
Scored between 0 - 1000

STATUS
- Open 8
- Ignored 0

LANGUAGES
- PHP 8

VULNERABILITY TYPES
- Use of Password Hash ... 7
- Server-Side Request For... 1

8 of 8 issues
Group by none Sort by highest severity

H Server-Side Request Forgery (SSRF)

SNYK CODE | CWE-918

SCORE 763

```
259     curl_setopt($ch, CURLOPT_HTTPHEADER, $array_headers);
260
261
262     if( !($this->result = curl_exec($ch)) )
```

Unsanitized input from *an HTTP parameter flows* into *curl_exec*, where it is used as an URL to perform a request. This may result in a Server-Side Request Forgery vulnerability.

lets-encrypt/integrations/directadmin/**httpsocket.php** 8 steps in 1 file

Ignore | Learn how to fix this issue

L Use of Password Hash With Insufficient Computational Effort

SNYK CODE | CWE-916

SCORE 438

```
49      $this->_account = $account;
50      $this->_subjects = $subjects;
51
52      $this->_identifier = $this->_getAccountIdentifier($account) . DIRECTORY
53          'order_' . md5(implode('|', $subjects));
```

MD5 hash (used in *md5*) is insecure. Consider changing it to a secure hashing algorithm.

lets-encrypt/vendor/fbett/le_acme2/src/LE_ACME2/**Order.ph...** 1 step in 1 file

Ignore | Learn how to fix this issue

Use of Password Hash With Insufficient Computational Effort

SNYK CODE | CWE-916

SCORE 438

```
1627    }
1628    switch ($action) {
1629        case 'vulnerabilities_test_notification':
1630            //creating a random string based on time.
1631            $random_string = md5( time() );
```

MD5 hash (used in *md5*) is insecure. Consider changing it to a secure hashing algorithm.

security/wordpress/**vulnerabilities.php** 1 step in 1 file

Learn about this type of vulnerability and how to fix it

Ignore | Learn how to fix this issue

Use of Password Hash With Insufficient Computational Effort

SNYK CODE | CWE-916

SCORE 438

```
81      {
82          if (get_option('rsssl_hashkey') && get_option('rsssl_hashkey') !== "")
83              $this->hash = get_option('rsssl_hashkey');
84          } else {
85              $this->hash = md5(uniqid(rand(), true));
```

MD5 hash (used in *md5*) is insecure. Consider changing it to a secure hashing algorithm.

security/wordpress/vulnerabilities/**FileStorage.php** 1 step in 1 file

Learn about this type of vulnerability and how to fix it

Ignore | Learn how to fix this issue

Use of Password Hash With Insufficient Computational Effort

SNYK CODE | CWE-916

SCORE 438

```
18          if ( $rsssl_folder ) {
19              $this->folderName = $this->folderName( $rsssl_folder );
20          } else {
21              $newFolderName    = 'really-simple-ssl/' . md5( uniqid( mt_rand(),
```

MD5 hash (used in *md5*) is insecure. Consider changing it to a secure hashing algorithm.

security/wordpress/vulnerabilities/**class-rsssl-folder-name.p...** 1 step in 1 file

Learn about this type of vulnerability and how to fix it

Ignore | Learn how to fix this issue

Use of Password Hash With Insufficient Computational Effort

SNYK CODE | CWE-916

SCORE 438

```
251         }
252         global $edd_plugin_url_available;
253
254         // Do a quick status check on this domain if we haven't already che
255         $store_hash = md5( $this->api_url );
```

MD5 hash (used in *md5*) is insecure. Consider changing it to a secure hashing algorithm.

upgrade/**upgrade-to-pro.php** 1 step in 1 file

Learn about this type of vulnerability and how to fix it

Ignore | Learn how to fix this issue

L Use of Password Hash With Insufficient Computational Effort

SNYK CODE | CWE-916

SCORE 438

```
50              $token = str_shuffle( time() );
51              update_option( 'rsssl_wp_version_token', $token );
52          }
53
54          $this->new_version = hash( 'md5', $token );
```

md5 hash (used in *hash*) is insecure. Consider changing it to a secure hashing algorithm.

security/wordpress/**hide-wp-version.php** 2 steps in 1 file

Learn about this type of vulnerability and how to fix it

Ignore | Learn how to fix this issue

L Use of Password Hash With Insufficient Computational Effort

SNYK CODE | CWE-916

SCORE 438

```
661     }
662
663     $timestamp = self::pack64( $step_count );
664
665     $hash = hash_hmac( $hash, $timestamp, $secret, true );
```

sha1 hash (used in *hash_hmac*) is insecure. Consider changing it to a secure hashing algorithm.