## ExpressionEngine <= 6.0.2 (Translate::save) PHP Code Injection Vulnerability

**• Software Link:**

https://expressionengine.com/

**• Affected Versions:**

Version 6.0.2 and prior versions.
Version 5.4.1 and prior versions.

**• Vulnerability Description:**

The vulnerable code is located in the “ExpressionEngine\Controller\Utilities\Translate::save()” method:

```
362  private function save($language, $file)
363  {
364
365      $file = ee()->security->sanitize_filename($file);
366
367      $dest_dir = $this->languages_dir . $language . '/';
368      $filename = $file . '_lang.php';
369      $dest_loc = $dest_dir . $filename;
370
371      $str = '<?php' . "\n" . '$lang = array(' . "\n\n\n";
372
373      ee()->lang->loadfile($file);
374
375      foreach ($_POST as $key => $val) {
376          $val = str_replace('<script', '', $val);
377          $val = str_replace('<iframe', '', $val);
378          $val = str_replace(array("\\", "'"), array("\\\\", "\'"), $val);
379
380          $str .= '\'' . $key . '\' => ' . "\n" . '\'' . $val . '\'' . ",\n\n";
381      }
382
383      $str .= "''=>''\n);\n\n";
384      $str .= "// End of File";
```

```
400  $this->load->helper('file');
401
402  if (write_file($dest_loc, $str)) {
403      ee('CP/Alert')->makeInline('shared-form')
404          ->asSuccess()
405          ->withTitle(lang('translations_saved'))
406          ->addToBody(sprintf(lang('file_saved'), $dest_loc))
407          ->defer();
```

User input passed via keys of POST parameters is not properly sanitized before being assigned to the “$str” variable at line 380. Such a variable will be used in a call to the “write_file()” function at line 402, trying to write user supplied content into the /system/user/language/[lang]/[file]_lang.php file. This can be exploited to inject and execute arbitrary PHP code. Successful exploitation of this vulnerability requires an account with permissions to access the CP translation system utilities.

**• Solution:**

Upgrade to version 6.0.3, 5.4.2, or later.

**• Disclosure Timeline:**

[03/02/2021] – Vendor notified through HackerOne
[15/02/2021] – Vulnerability acknowledged by the vendor
[16/02/2021] – CVE number assigned
[17/02/2021] – Version 6.0.3 released
[04/03/2021] – Version 5.4.2 released
[15/03/2021] – Public disclosure

**• CVE Reference:**

The Common Vulnerabilities and Exposures project (cve.mitre.org)
has assigned the name CVE-2021-27230 to this vulnerability.

**• Credits:**

Vulnerability discovered by Egidio Romano.

**• Other References:**

https://hackerone.com/reports/1093444