mariuszpoplwski / **CVE-2020-13443**

Last active 2 years ago

CVE-2020-13443

```
CVE-2020-13443

https://gist.github.com/mariuszpoplawski/703586aa068bdad21f2c098f396ce04f



----------------------------------------

[Suggested description]
 ExpressionEngine before 5.3.2 allows remote attackers to upload and execute arbitrary code in a .php%20 file via
 Compose Msg, Add attachment, and Save As Draft actions.
 A user with low privileges (member) is able to upload this.
 It is possible to bypass the MIME type check and
 file-extension check while uploading new files.
 Short aliases are not used for an attachment; instead, direct access is
 allowed to the uploaded files. It is possible to upload
 PHP only if one has member access, or registration/forum is enabled
 and one can create a member with the default group id of 5. To exploit this, one
 must to be able to send and compose messages (at least).

 ----------------------------------------

 [Additional Information]
 To trigger the vulnerability we can use messages composer
 http://127.0.0.1/index.php/member/messages/compose

 Affected function
 "Compose msg" - add attachment - "save as draft"

 Files attached to message and saved as draft are stored in
 /var/www/html/images/pm_attachments/$FILE_NAME - Accesable from web app root folder.

 http://127.0.0.1/images/pm_attachments/$UPLOADED_FILE_NAME.EXT

 We were able to send file name "POC.php%20" it was valid PNG file with PHP code inside. below we present te PoC.

 Quick overview of code
 Global variable in CMS by default $this-blacklisted_extensions =

 (
     [0] = php
     [1] = php3
     [2] = php4
     [3] = php5
     [4] = php7
     [5] = phps
     [6] = phtml
 )
 /system/ee/legacy/libraries/Upload.php code at line 532
 If we send file that is not in blacklisted_extensions array for example ".php%20", our upload will be successful.

 if (in_array($ext, $this-blacklisted_extensions))
        {
            return FALSE;
        }
 /system/ee/EllisLab/ExpressionEngine/Library/Mime/MimeType.php
 To upload our file "MimeType" have to be in white list also, so we uploaded PNG file with PHP code in comment TAG.

 Line 237:   public function isSafeForUpload($mime)
     {
         return in_array($mime, $this-whitelist, TRUE);
     }
 ...
 Line 95:    public function ofFile($path){
 ...
 Line 105: $finfo = finfo_open(FILEINFO_MIME_TYPE);
 /system/ee/legacy/libraries/Upload.php code at
 Function clean_file_name is called after check ...

 ----------------------------------------

 [VulnerabilityType Other]
 low privileged user PHP file upload led to Remote Command Execution

 ----------------------------------------

 [Vendor of Product]
 obfuscode

 ----------------------------------------

 [Affected Product Code Base]
```

```
expressionengine.com - before 5.3.2

----------------------------------------

[Affected Component]
member/messages/compose

----------------------------------------

[Attack Type]
Remote

----------------------------------------

[Impact Code execution]
true

----------------------------------------

[Attack Vectors]
User with low privileges have to upload file during messages composer process. File extension check and be bypassed using %20 at the end o

----------------------------------------

[Discoverer]
Mariusz Poplawski (afine.pl)

----------------------------------------

[Reference]
https://expressionengine.com/blog


Mariusz Popławski / AFINE.com team
```