jinhuang1102 / CVE-ID-Reports Public

Code Issues Pull requests Actions Projects Security Insights

e4c33529b2 ▾ ···

CVE-ID-Reports / Easy Form Builder.md

jinhuang1102 Update Easy Form Builder.md History

1 contributor

35 lines (29 sloc) | 1.59 KB ···

Easy Form Builder <= 1.0 - Arbitrary File Upload

Easy Form Builder 1.0 is a free plugin designed to provide a highly customized form to the plugin user, and allow the user with admin privilege to create a registration page for the visitor. in order to provide the functionality, it uses a publicly accessible AJAX function, EFBP_verify_upload_file_callback.

```
<?php
function EFBP_verify_upload_file_callback()
{
    $total = count($_FILES['file']['name']);
    $upload_dir = wp_upload_dir();
    $uploadFolderPath = $upload_dir['basedir']; // this will make uploads folder in the wp-content. it will be outside the plugin fol

    // Loop through each file
    for ($i = 0; $i < $total; $i++) {
        if ($_FILES['file']['tmp_name'][$i] != "") {
            //Setup our new file path
            $newFilePath = $uploadFolderPath . "/formbuilder/" . $_FILES['file']['name'][$i];
            //Upload the file into the temp dir
            if (move_uploaded_file($_FILES['file']['tmp_name'][$i], $newFilePath)) {
                echo $i . ". " . $newFilePath . " <br> ";
            }
        }
    }
    wp . die();
}
```

While the developer tired to limit the file upload types, he or she doesn't solve this problem correctly. The developer provides a list of file types to "Block" or "Only Allow" the uploaded files, but this list doesn't block the .php file.

image

As a result, File with .php (executable) extension will be stored in the local directory, `wp_upload_dir()/formbuilder/` , without any restriction.