beerpwn update readme ... on Apr 19, 2020 History

..	
screen	2 years ago
CVE-2020-10564_exploit.py	2 years ago
readme.md	2 years ago
report.md	2 years ago
report.pdf	2 years ago

readme.md

CVE-2020-10564

Author: p4w

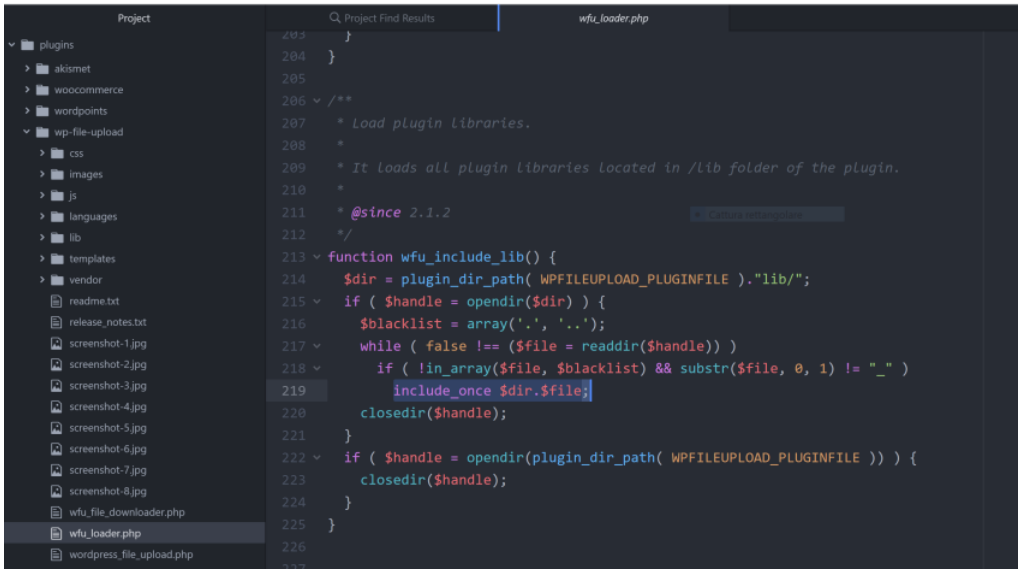
Twitter: https://twitter.com/p4w16

HTB: https://www.hackthebox.eu/profile/32300

e-mail: riccardo.krauter@gmail.com

- plugin url: https://wordpress.org/plugins/wp-file-upload/#developers
- fixed version 4.13.0
- CVE-2020-10564 (Directory Traversal on WP File Upload to RCE)

The vulnerability affecting the plugin let a user gain **Remote Code Execution** by uploading a simple `.jpg` or `.txt` file by abusing a **directory traversal**.
WordPress File Upload is a plugin for **WordPress**. I manage to find a directory traversal vuln. on the file upload functionality. It's possible to use this vulnerability to gain RCE by uploading a file (doesn't matter the extension) inside the `lib` directory of the plugin. The RCE can be triggered from an unathenticated user, also it doesn't require any admin interaction.
Why this work?
Well, thnx to this:



this piece of code shows that the function `wfu_include_lib()` will `include_once` all the file in the `lib` directory (extension does not matter). Then we can use the **path traversal** to wrtite a file inside that directory to **gain RCE**. This function will be called automatically every time the plugin is present in a page by the init page (you can check the file `wfu_loader.php`).
Here you can find the report that I shared with the mainteiner of the plugin, inside it you can find the PoC to reproduce the issue.
Here you can find a simple python script exploit. Example usage:

```
$ python exploit.py http://localhost/wordpress/test-wp-file-upload-plugin/ /wordpress
```

Enjoy the own4ge.

Cheers, p4w