New issue

Jump to bottom

phpinfo (phpinfo.php) shows PHP information including values of HttpOnly cookies. #567

Closed jhhua opened this issue on Aug 11, 2021 · 5 comments

jhhua commented on Aug 11, 2021

All 0.9.x versions (prior to 0.9.16), are affected.
System Information Leak (phpinfo()) vulnerability in flextype 0.9.16 via the phpinfo() parameter to 1) flextype/vendor/phpfastcache/phpfastcache/docs/examples/phpinfo.php ,2) flextype/vendor/phpfastcache/phpfastcache/docs/examples/index.php

it's allows remote attackers to obtain configuration information via a phpinfo action in a request to phpinfo.php、index.php, which calls the phpinfo function.

Awilum commented on Aug 12, 2021 Member

Access to vendor folder is closed here:
https://github.com/flextype/flextype/blob/master/.htaccess#L56

And you can't access here:
https://flextype.org/vendor/phpfastcache/phpfastcache/docs/examples/phpinfo.php
https://flextype.org/vendor/phpfastcache/phpfastcache/docs/examples/index.php

jhhua commented on Aug 12, 2021 Author

thanks, i found this vulnerability it's between 0.9.12 and 0.9.16 via,it's not very dangerious

Awilum closed this as completed on Aug 12, 2021

Geolim4 commented on Aug 12, 2021

Hello,

I have been notified today by mail of a potential vulnerability in Phpfastcache, I take this alert very seriously and working on it to push a fix tonight along with a CVE if needed.

This code is a very old code (2016) located in /docs directory that should not be here.

Thanks you.

👍 1

Awilum commented on Aug 12, 2021 Member

@Geolim4 Thanks!

Geolim4 commented on Aug 12, 2021

A CVE has been released and published here: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37704

Thanks :D

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants