New issue

Jump to bottom

PHP arbitrary file include #2762

Closed **bstapes** opened this issue on Apr 2, 2020 · 3 comments

bstapes commented on Apr 2, 2020 • edited

Teampass allows users to choose from several different languages. The user changes their language preference by sending a POST request to Teampass (`/teampass/sources/users.queries.php`) that contains the string of the language they choose ("english", "spanish", etc). This string provided by the user is not validated or sanitized in any way.

After the string provided by the user is stored in the DB, it is eventually used in `core.php` during login on line 78:
`require_once $SETTINGS['cpassman_dir'].'/includes/language/'.$_SESSION['user_language'].'.php';`

This allows any user to file_include any existing PHP file on disk. If a user could upload their own PHP file, then it could be combined with this bug to achieve code execution on the Teampass server.

Steps to reproduce
Send a POST request to change user language, but modify the value of the `newValue` parameter to a value of your choosing (eg: `../backups/script.backup`).

```
POST /teampass/sources/users.queries.php HTTP/1.1
Host: localhost
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://localhost/teampass/index.php?page=items
Cookie: <cookie>;
KEY_PHPSESSID=<value>;
PHPSESSID=<value>;
jstree_select=2

newValue=Spanish&id=userlanguage_10000004&<cookie>
```

Log out and log back in to force the TeamPass server to read the PHP file of your choosing.

Steps to fix

- Validate the value from the "newValue" parameter. The only permissible values should be a hard-coded list of strings that exist in /includes/language/ directory EG: `$validLanguages = array('arabic', 'bulgarian', 'etc');` .
- In the case of a non-valid value, Teampass should deny the language change and immediately stop processing the data in the newValue parameter. This validation could potentially occur here, where the `userlanguage` parameter is processed.

Server configuration

Teampass version:
2.1.27.36

sata-sa commented on May 8, 2020

Hey! In steps to fix are you able to provide more details?

- In which file can be this hardcoded?
- After the "hardcoded" values will be this archived automatically?

bstapes commented on May 8, 2020 Author

@sata-sa I updated the steps to fix with a bit more information. Does that help?

> After the "hardcoded" values will be this archived automatically?

I'm not sure what you mean. Are you asking if this issue could be closed after the `userlanguage` parameter is validated against a list of acceptable values? Then yes, that is all that is needed here.

sata-sa commented on May 8, 2020 • edited

@bstapes It does!

Thanks for your quick support.

👍 1

bigio mentioned this issue on Feb 5, 2021

Issue 2762 #2874

Closed

nilsteampassnet closed this as completed on Oct 31

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants