New issue

Jump to bottom

Bypass authentication through loose comparison #668

Closed **peng-hui** opened this issue on May 26, 2020 · 2 comments

peng-hui commented on May 26, 2020

[lists/index.php:145]

phplist3/public_html/lists/index.php
Line 145 in d0a0107

```
145      $encP == $userpassword && $_POST['email'] == $emailcheck;
```

has the potential of authentication bypass problem through loose comparison. (==).

Here is another [example].

phplist3/public_html/lists/index.php
Line 148 in d0a0107

```
148      $canlogin = $_POST['password'] == $userpassword && $_POST['email'] == $emailcheck;
```

A similar CVE can be found CVE-2020-8547 and here

In addition, in

phplist3/public_html/lists/admin/subscribelib2.php
Line 143 in d0a0107

```
143      if (empty($_POST['password']) || $_POST['password'] != $_POST['password_check']) {
```

It also uses a loose comparison. The functionality might not perform correctly for the password rechecking in the magic strings cases. For example, "0e11" and "0e22" shall be equal under loose comparison, but actually they are not.

suelaP commented on May 26, 2020 Member

Hi **@peng-hui** ,
Thanks for the report, would you be willing to submit a pull request with the fix?

michieldl commented on May 26, 2020 Member

Resolved with `def1cee`

michieldl closed this as completed on May 26, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants