New issue

Jump to bottom

Injection SQL sur le cookie user_id #51

Closed **h4knet** opened this issue on Feb 26, 2020 · 1 comment

Assignees

Labels bug

h4knet commented on Feb 26, 2020

Bonjour,

Il est possible de réaliser une injection SQL sur le cookie `user_id` . Il a été observé que cette injection est possible sur les pages `index.php` , `login.php` et `logout.php` sans authentification préalable.

Exemple d'injection de code utilisant la fonction sleep(3):

```
Cookie: user_id=1' union select sleep(3) -- ;
```

L'exploitation d'une telle injection SQL peut permettre à un attaquant d'obtenir des accès administrateurs sur l'application (récupération de session_id admin, dump de table users).

Ceci a été testé sur une installation de EON **5.1** et **5.3** téléchargée à partir du site officiel (la 5.2 doit probablement aussi être vulnérable).

Le fichier source permettant l'injection SQL est `eonweb/include/classes/Translator.class.php` au morceau de code suivant :

```
// Check if user default lang is defined
if(isset($_COOKIE['user_id'])){
                $lang = mysqli_result(sqlrequest($database_eonweb,"select user_language from users where user_id='".$_COOKIE['user_id']."'"),0);
}
```

davoult self-assigned this on Feb 27, 2020

CorrochanoDavid pushed a commit that referenced this issue on Feb 27, 2020

`issue #51 injection SQL in Cookie` de8e206

davoult added a commit that referenced this issue on Feb 28, 2020

`Merge pull request #52 from EyesOfNetworkCommunity/issue51` ··· ba82675

davoult added the bug label on Feb 28, 2020

davoult commented on Feb 28, 2020 Contributor

Encore une fois merci **@h4knet** pour cette remontée de vulnérabilité.
Le correctif a été publié dans eonweb-5.3-3.x86_64.rpm.

davoult closed this as completed on Feb 28, 2020

OscarPoels mentioned this issue on Nov 30, 2020

Multiples vulnérabilités critiques (Score CVSS v3 = 9.8) #76

Closed

Assignees

davoult

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants