

[New issue](#)[Jump to bottom](#)

Possible XSS vulnerability #156

Closedenferas opened this issue on Apr 6 · 5 comments · Fixed by [#173](#)

Labels

bug

enferas commented on Apr 6

Hello,

I would like to report for XSS vulnerability.

In file <https://github.com/MoeNetwork/Tieba-Cloud-Sign/blob/master/templates/control.php> line 53.

```
case 'setplug':  
    $plug = strip_tags($_GET['plug']);  
    $plugininfo = getPluginInfo($plug);
```

Then, there is an echo in line 62.

```
echo '<a href="'. $plugininfo['plugin']['url']. ' " target="_blank">';
```

strip_tags is not secure in this case. If you can look to this code example the alert will be printed when you press on the link.

```
<?php  
$x = "'javascript:alert()'";  
$y = strip_tags($x);  
echo "<a href=$x>ClickMe</a>";
```

BANKA2017 commented on Apr 6

Collaborator[Tieba-Cloud-Sign/templates/control.php](#)

Line 23 in e13aa6e

```
23      if (ROLE != 'admin') msg('权限不足!');
```

[Tieba-Cloud-Sign/lib/plugins.php](#)

Lines 197 to 199 in e13aa6e

```
197      if (!file_exists($path . $plugin . '.php')) {
198          return false;
199      }
```

这是一个没有想象中严重的漏洞，我们在前面设置了权限检查挡住了非admin用户的访问，此外文件存在性检查会确保不存在的插件不会被加载，因此触发这个漏洞的需要：

- 用户为**管理员**
- 使用了带有恶意外部链接的插件

感谢您的反馈，我们将会在晚些时候进行修复

translated by deepl.com

[Tieba-Cloud-Sign/templates/control.php](#)

Line 23 in e13aa6e

```
23      if (ROLE != 'admin') msg('权限不足!');
```

[Tieba-Cloud-Sign/lib/plugins.php](#)

Lines 197 to 199 in e13aa6e

```
197      if (!file_exists($path . $plugin . '.php')) {
198          return false;
199      }
```

This is not as serious a vulnerability as you might think, we set up a permission check earlier to block access by non-admin users, in addition the file existence check will ensure that non-existent plugins will not be loaded, so two conditions are required to trigger this vulnerability

- The user is an **administrator**
- A plugin with a malicious url is used

Thank you for your feedback, we will fix it later

  kenvix added the `bug` label on Apr 7

RiotGamesU commented on May 15

[Tieba-Cloud-Sign/templates/control.php](#)

Line 23 in e13aa6e

```
23      if (ROLE != 'admin') msg('权限不足!');
```

[Tieba-Cloud-Sign/lib/plugins.php](#)

Lines 197 to 199 in e13aa6e

```
197      if (!file_exists($path . $plugin . '.php')) {  
198          return false;  
199      }
```

这是一个没有想象中严重的漏洞，我们在前面设置了权限检查挡住了非admin用户的访问，此外文件存在性检查会确保不存在的插件不会被加载，因此触发这个漏洞的需要：

- 用户为**管理员**
- 使用了带有恶意外部链接的插件

感谢您的反馈，我们将会在晚些时候进行修复

translated by deepl.com

[Tieba-Cloud-Sign/templates/control.php](#)

Line 23 in e13aa6e

```
23      if (ROLE != 'admin') msg('权限不足!');
```

[Tieba-Cloud-Sign/lib/plugins.php](#)

Lines 197 to 199 in e13aa6e

```
197      if (!file_exists($path . $plugin . '.php')) {  
198          return false;  
199      }
```

This is not as serious a vulnerability as you might think, we set up a permission check earlier to block access by non-admin users, in addition the file existence check will ensure that non-existent plugins will not be loaded, so two conditions are required to trigger this vulnerability

- The user is an **administrator**
- A plugin with a malicious url is used

Thank you for your feedback, we will fix it later

礼貌问询deepl.com中译英和英译中效果怎么样

n0099 commented on May 16

Collaborator

礼貌问询deepl.com中译英和英译中效果怎么样

您已经看到了

enferas commented on Jun 13

Author

[CVE-2022-28920](#) is assigned for this vulnerability.
Thank you.

n0099 commented on Jun 13

Collaborator


This is the first CVE assigned to tc in its seven years history.



🔖  n0099 linked a pull request on Jun 14 that will close this issue

尝试修复 'CVE-2022-28920' #173

 Merged

 n0099 closed this as completed on Jun 14

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 尝试修复 'CVE-2022-28920'
kdnetwork/Tieba-Cloud-Sign

5 participants

