



# CVE-2021-36858

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-36858
<b>State</b>	PUBLIC
<b>Assigner</b>	audit@patchstack.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-10-28 16:15:00 UTC
<b>Updated</b>	2022-10-28 18:44:00 UTC
<b>Description</b>	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Themepoints Testimonials plugin <= 2.6 on WordPress.

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Themepoints	Testimonials	All	All	All	All

## References

Reference	Source	Link	Ta
Testimonials – WordPress plugin   WordPress.org	CONFIRM	<a href="https://wordpress.org">wordpress.org</a>	
WordPress Testimonials plugin <= 2.6 - Auth. Stored Cross-Site Scripting (XSS) vulnerability - Patchstack	CONFIRM	<a href="https://patchstack.com">patchstack.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	ca
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	ca

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Vulnerability discovered by Ngo Van Thien (Patchstack Alliance)

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**