CVE-2021-24873

Published on: 11/23/2021 12:00:00 AM UTC
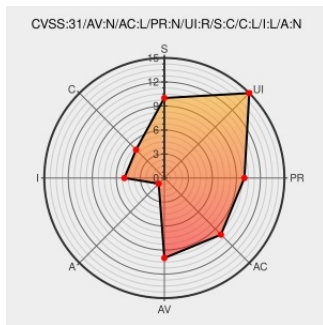
Last Modified on: 11/24/2021 04:36:00 PM UTC

CVE-2021-24873

Source: Mitre | Source: Nist | Print: PDF

Certain versions of Tutor Lms from Themeum contain the following vulnerability:

The Tutor LMS WordPress plugin before 1.9.11 does not sanitise and escape user input before outputting back in attributes in the Student Registration page, leading to a Reflected Cross-Site Scripting issue

CVE-2021-24873 has been assigned by ☁ contact@wpscan.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: ☁ **Unknown** - **Tutor LMS – eLearning and online course solution** version **< 1.9.11**

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Attention Required! | Cloudflare	wpscan.com text/html Inactive Link Not Archived	☁ MISC wpscan.com/vulnerability/19980b57-1954-4a29-b2c2-43eadf758ed3

403 Forbidden	**plugins.trac.wordpress.org** **text/html** **Inactive Link** **Not Archived**	Ⓦ CONFIRM plugins.trac.wordpress.org/changeset/2615802/tutor

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Themeum	Tutor Lms	All	All	All	All

cpe:2.3:a:themeum:tutor_lms:*:*:*:*:*:wordpress:*:*:

Discovery Credit

JrXnm

Social Mentions

Source	Title	Posted (UTC)
🐦 @LinInfoSec	Wordpress - CVE-2021-24873: plugins.trac.wordpress.org/changeset/2615…	2021-11-23 21:36:17

← Previous ID   Next ID→