



WordPress Tutor LMS Plugin <= 2.1.10 is vulnerable to SQL Injection

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

Summary

CVE	CVE-2023-25990
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-03 17:15:08 UTC
Updated	2026-04-28 19:19:54 UTC
Description	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LM

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-89 | CWE-89 CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	audit@patchstack.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Themeum	Tutor LMS	affected n/a 2.1.10 custom	Not specified
ADP	Themeum	Tutor Lms	affected 2.1.10 custom	Not specified

References

Reference	Source
WordPress Tutor LMS plugin <= 2.1.10 - Multiple Tutor Instructor+ SQL Injection vulnerability - Patchstack	af854a3a-2127-422b-91ae-364d
patchstack.com/database/Wordpress/Plugin/tutor/vulnerability/wordpress-tutor...	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Rafie Muhammad (Patchstack) (en)

Additional Advisory Data

Solutions

CNA: Update to 2.2.0 or a higher version.

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

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report