WordPress Open edX LMS plugin <= 2.6.1 - Reflected Cross Site Scripting (XSS) vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-52452
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-02 14:15:06 UTC
Updated	2026-04-28 19:27:34 UTC
Description	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in eduNEXT Open edX L

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from audit@patchstack.com

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

EPSS: 0.001970000 probability, percentile 0.414480000 (date 2026-04-28)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	EduNEXT	Open EdX LMS	affected n/a 2.6.1 custom	Not specified

References

Reference
patchstack.com/database/wordpress/plugin/edunext-openedx-integrator/vulnerab...
https://patchstack.com/database/wordpress/plugin/edunext-openedx-integrator/vulnerability/wordpress-open-edx-lms-plugin-2-6-1-reflected-cr
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: Mika (Patchstack Alliance) (en)

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