



CVE-2022-2034

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

Summary

CVE	CVE-2022-2034
State	PUBLIC
Assigner	contact@wpscan.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-29 18:15:00 UTC
Updated	2023-11-07 03:46:00 UTC
Description	The Sensei LMS WordPress plugin before 4.5.0 does not have proper permissions set in one of its REST endpoint, allowing

Risk And Classification

Problem Types: CWE-639

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Automattic	Sensei Lms	All	All	All	All

References

Reference	Source	Link
HackerOne	MISC	hackerone
Sensei LMS < 4.5.0 - Unauthenticated Private Messages Disclosure via Rest API WordPress Security Vulnerability	MISC	wpscan.co
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

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

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