CVE-2022-38974

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

Summary

CVE	CVE-2022-38974
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-18 19:15:00 UTC
Updated	2022-11-21 13:32:00 UTC
Description	Broken Access Control vulnerability in WPML Multilingual CMS premium plugin <= 4.5.10 on WordPress allows users with s

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wpml	Wpml	All	All	All	All

References

Reference	Source	Link
WordPress WPML Multilingual CMS premium plugin <= 4.5.10 - Broken Access Control vulnerability - Patchstack	CONFIRM	patchstack.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Vulnerability discovered by Dave Jong (Patchstack)

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

Free CVE JSON API cve.report/api

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