Theme and plugin translation for Polylang <= 3.2.16 - Missing Authorization

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

Summary

CVE	CVE-2022-4169
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-11-28 18:15:12 UTC
Updated	2026-04-08 18:17:32 UTC
Description	The Theme and plugin translation for Polylang is vulnerable to authorization bypass in versions up to, and including, 3.2.16

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
3.1	security@wordfence.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L
3.1	CNA	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

Low

vailability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Editio
Application	Theme And Plugin Translation For Polylang Project	Theme And Plugin Translation For Polylang	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Marcinkazmierski	Theme And Plugin Translation For Polylang TTfP	affected 3.2.16 semver	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/9f6a358a-333c-4eb7-9149-348bf...	security@wordfence.com	www.wor
Vulnerability Advisories Continued - Wordfence	af854a3a-2127-422b-91ae-364da2661108	www.wor
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	plugins.tr
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: Florent BESNARD (en)

Additional Advisory Data

Source	Time	Event
CNA	2022-11-28T00:00:00.000Z	Disclosed

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**