WordPress Owl Carousel plugin <= 0.5.3 - Broken Access Control vulnerability

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

Summary

CVE	CVE-2022-44578
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-12-13 15:15:07 UTC
Updated	2026-04-28 19:18:53 UTC
Description	Missing Authorization vulnerability in Pierre JEHAN Owl Carousel allows Exploiting Incorrectly Configured Access Control S

Risk And Classification

Primary CVSS: v3.1 5.3 MEDIUM from audit@patchstack.com

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

EPSS: 0.001490000 probability, percentile 0.349330000 (date 2026-05-12)

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Pierre JEHAN	Owl Carousel	affected n/a 0.5.3 custom	Not specified

References

Reference
patchstack.com/database/wordpress/plugin/owl-carousel/vulnerability/wordpres...
https://patchstack.com/database/wordpress/plugin/owl-carousel/vulnerability/wordpress-owl-carousel-plugin-0-5-3-broken-access-control-csrf-
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

CNA: thiennv (Patchstack Alliance) (en)

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