



WordPress Shiprocket plugin <= 2.0.8 - Insecure Direct Object References (IDOR) vulnerability

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

Summary

CVE	CVE-2025-68051
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-20 16:22:09 UTC
Updated	2026-04-27 19:16:23 UTC
Description	Authorization Bypass Through User-Controlled Key vulnerability in Shiprocket Shiprocket shiprocket allows Exploiting Incon

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from audit@patchstack.com

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

EPSS: 0.000380000 probability, percentile 0.114600000 (date 2026-04-27)

Problem Types: CWE-639 | CWE-639 Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Shiprocket	Shiprocket	affected 2.0.8 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/shiprocket/vulnerability/wordpress-...	audit@patchstack.com	patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, and

Vendor Comments And Credit

Discovery Credit

CNA: NumeX | Patchstack Bug Bounty Program (en)

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