



WordPress Official Integration for Billingo plugin <= 4.3.0 - Privilege Escalation vulnerability

[MITRE](#)

[NVD](#)

[CVE.ORG](#)

[JSON API](#)

[Print: PDF](#)

Summary	
CVE	CVE-2025-49950
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-22 15:15:41 UTC
Updated	2026-04-27 20:16:18 UTC
Description	Missing Authorization vulnerability in billingo Official Integration for Billingo billingo allows Privilege Escalation.This issue aff

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from audit@patchstack.com

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

EPSS: 0.000190000 probability, percentile 0.051740000 (date 2026-04-27)

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Bilingo	Official Integration For Bilingo	affected 4.3.0 custom	Not specified

References

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

Vendor Comments And Credit

Discovery Credit

CNA: Martino Spagnuolo (r3verii) | Patchstack Bug Bounty Program (en)

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