



WordPress WPSubscription plugin <= 1.8.10 - Insecure Direct Object References (IDOR) vulnerability

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

Summary

CVE	CVE-2025-69347
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 17:16:27 UTC
Updated	2026-04-24 16:32:53 UTC
Description	Authorization Bypass Through User-Controlled Key vulnerability in Convers Lab WPSubscription subscription allows Explo

Risk And Classification

Primary CVSS: v3.1 8.5 HIGH from ADP

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

EPSS: 0.000320000 probability, percentile 0.091510000 (date 2026-04-23)

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

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N
3.1	audit@patchstack.com	Secondary	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N
3.1	CNA	CVSS	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality
High
Integrity
Low
Availability
None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Convers Lab	WPSubscription	affected 1.8.10 custom	Not specified

References

Reference	Source	Link	Tags
patchstack.com/database/Wordpress/Plugin/subscription/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: Jitlada | Patchstack Bug Bounty Program (en)

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