



# WordPress wpDiscuz Plugin <= 7.6.3 is vulnerable to Insecure Direct Object References (IDOR)

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

## Summary

<b>CVE</b>	CVE-2023-46311
<b>State</b>	PUBLISHED
<b>Assigner</b>	Patchstack
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-12-20 14:15:20 UTC
<b>Updated</b>	2026-04-28 19:21:42 UTC
<b>Description</b>	Authorization Bypass Through User-Controlled Key vulnerability in gVectors Team Comments – wpDiscuz. This issue affects

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from nvd@nist.gov

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

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N
3.1	audit@patchstack.com	Secondary	2.7	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	2.7	LOW	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

High

Integrity

High

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gvectors	Wpdiscuz	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GVectors Team	Comments WpDiscuz	affected n/a 7.6.3 custom	Not specified

### References

Reference	Source	Link
patchstack.com/database/vulnerability/wpdiscuz/wordpress-wpdiscuz-plugin-7-6...	af854a3a-2127-422b-91ae-364da2661108	patchstack.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Revan Arifio (Patchstack Alliance) (en)

### Additional Advisory Data

#### Solutions

**CNA:** Update to 7.6.4 or a higher version.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)