WordPress Curly theme <= 3.3 - Insecure Direct Object References (IDOR) vulnerability

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

Summary

CVE	CVE-2026-22393
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-01-22 17:16:32 UTC
Updated	2026-04-28 19:36:34 UTC
Description	Authorization Bypass Through User-Controlled Key vulnerability in Mikado-Themes Curly curly allows Exploiting Incorrectly

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from audit@patchstack.com

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

EPSS: 0.000370000 probability, percentile 0.110820000 (date 2026-04-28)

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

Version	Source	Type	Score	Severity	Vector
3.1	audit@patchstack.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L
3.1	CNA	CVSS	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mikado-Themes	Curly	affected 3.3 custom	Not specified

References

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

Vendor Comments And Credit

Discovery Credit

CNA: Tran Nguyen Bao Khanh (VCI - VNPT Cyber Immunity) | Patchstack Bug Bounty Program (en)

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