



WordPress TheGem theme < 5.8.1.1 - Broken Access Control vulnerability

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

Summary

CVE	CVE-2023-32238
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-30 00:15:50 UTC
Updated	2026-04-28 19:20:25 UTC
Description	Vulnerability in CodexThemes TheGem (Elementor), CodexThemes TheGem (WPBakery).This issue affects TheGem (Eler

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:L/I:L/A:N

EPSS: 0.000780000 probability, percentile 0.230550000 (date 2026-04-28)

Problem Types: CWE-284 | CWE-284 CWE-284 Improper Access Control

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:L/I:L/A:N
3.1	CNA	CVSS	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	CodexThemes	TheGem Elementor	affected n/a 5.8.1.1 custom	Not specified
CNA	CodexThemes	TheGem WPBakery	affected n/a 5.8.1.1 custom	Not specified

References

Reference	Source	Link	Tags
vdp.patchstack.com/database/wordpress/theme/thegem-elementor/vulnerability/wordpress-5.8.1.1-cve-2024-10000	audit@patchstack.com	vdp.patchstack.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

Vendor Comments And Credit

Discovery Credit

CNA: Dave Jong | Patchstack Threat Intelligence (en)

Additional Advisory Data

Solutions

CNA: Update the WordPress TheGem (Elementor) theme to the latest available version (at least 5.8.1.1).

CNA: Update the WordPress TheGem (WPBakery) theme to the latest available version (at least 5.8.1.1).

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

CVE.report and Source URL Uptime Status status.cve.report