



# Gutenberg Blocks by Kadence Blocks – Page Builder Features <= 3.1.26 - Authenticated(Contributor+) Server-Side Request Forgery (SSRF)

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

## Summary

<b>CVE</b>	CVE-2023-6964
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-04-09 19:15:13 UTC
<b>Updated</b>	2026-04-08 19:19:03 UTC
<b>Description</b>	The Gutenberg Blocks by Kadence Blocks – Page Builder Features plugin for WordPress is vulnerable to Server-Side Request Forgery (SSRF) via an authenticated contributor user. An attacker can exploit this vulnerability to perform a Server-Side Request Forgery (SSRF) attack against an internal service, such as a local host or a private IP address, and potentially access sensitive information or perform actions on the internal network.

## Risk And Classification

**Primary CVSS:** v3.1 6.4 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.003430000 probability, percentile 0.569530000 (date 2026-04-22)

**Problem Types:** CWE-918 | CWE-918 CWE-918 Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	security@wordfence.com	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	DECLARED	8.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kadencewp	Gutenberg Blocks With Ai	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Stellarwp	Kadence Blocks Page Builder Toolkit For Gutenberg Editor	affected 3.1.26 semver	Not specified

### References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/b01ad77f-2349-48bb-b4e9-f7cbc...	af854a3a-2127-422b-91ae-364da2661108	www.wor
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	plugins.tr
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

### Vendor Comments And Credit

Discovery Credit

**CNA:** Lucio Sá (en)

### Additional Advisory Data

Source	Time	Event
CNA	2023-12-19T00:00:00.000Z	Vendor Notified
CNA	2024-04-09T00:00:00.000Z	Disclosed

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

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)