WordPress Starter Templates Plugin <= 3.2.4 is vulnerable to Server Side Request Forgery (SSRF)

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

Summary

CVE	CVE-2023-41804
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-12-07 11:15:07 UTC
Updated	2026-04-28 19:21:19 UTC
Description	Server-Side Request Forgery (SSRF) vulnerability in Brainstorm Force Starter Templates — Elementor, WordPress & Beav

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from nvd@nist.gov

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

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	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	7.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:N/AC:H/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

Unchanged

Confidentiality

Low

ntegrity

Low

vailability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Brainstormforce	Starter Templates	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Brainstorm Force	Starter Templates Elementor WordPress Beaver Builder Templates	affected n/a 3.2.4 custom	Not specified

References

Reference	Source
WordPress Starter Templates plugin <= 3.2.4 - Server Side Request Forgery (SSRF) vulnerability - Patchstack	af854a3a-2127-422b-91ae-3
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Rafie Muhammad (Patchstack) (en)

Additional Advisory Data

Solutions

CNA: Update to 3.2.5 or a higher version.

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

Free CVE JSON API cve.report/api

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