BUKAZU Search widget <= 3.3.2 - Authenticated (Contributor+) Stored Cross-Site Scripting via 'shortcode' Shortcode Attribute

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

Summary

CVE	CVE-2025-13840
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-12 04:15:42 UTC
Updated	2026-04-08 19:23:29 UTC
Description	The BUKAZU Search widget plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'shortcode' paramete

Risk And Classification

Primary CVSS: v3.1 6.4 MEDIUM from security@wordfence.com

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

EPSS: 0.000550000 probability, percentile 0.173670000 (date 2026-04-13)

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Bobvanoorschot	Bukazu Search Widget	affected 3.3.2 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset/3427947	security@wordfence.com	plugins.trac.wordpress.
plugins.trac.wordpress.org/browser/bukazu-search-widget/tags/3.3.2/bukazu-widget.php	security@wordfence.com	plugins.trac.wordpress.
plugins.trac.wordpress.org/browser/bukazu-search-widget/trunk/bukazu-widget.php	security@wordfence.com	plugins.trac.wordpress.
www.wordfence.com/threat-intel/vulnerabilities/id/a666d0e4-4fa7-4794-b270-afbcc...	security@wordfence.com	www.wordfence.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Gilang Asra Bilhadi (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-11T14:31:53.000Z	Disclosed

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**