Block Logic <= 1.0.8 - Authenticated (Contributor+) Remote Code Execution

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

Summary

CVE	CVE-2025-2303
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-03-22 07:15:24 UTC
Updated	2026-04-08 18:24:34 UTC
Description	The Block Logic – Full Gutenberg Block Display Control plugin for WordPress is vulnerable to Remote Code Execution in al

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from security@wordfence.com

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

EPSS: 0.012950000 probability, percentile 0.796830000 (date 2026-04-08)

Problem Types: CWE-94 | CWE-94 CWE-94 Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Landwire	Block Logic Full Block Display Control	affected 1.0.8 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset/3430763	security@wordfence.com	plugins.trac.wordpress.org
plugins.trac.wordpress.org/browser/block-logic/tags/1.0.8/block-logic.php	security@wordfence.com	plugins.trac.wordpress.org
www.wordfence.com/threat-intel/vulnerabilities/id/4a76f851-3f4e-4457-a33c-eede5...	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: Oliver Campion (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-03-11T00:00:00.000Z	Discovered
CNA	2025-03-21T17:53:40.000Z	Disclosed

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

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