WordPress Header Builder Plugin – Pearl <= 1.3.6 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode

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

Summary

CVE	CVE-2024-4000
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-02 17:15:33 UTC
Updated	2026-04-08 19:21:30 UTC
Description	The WordPress Header Builder Plugin – Pearl plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plug

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: 0.003090000 probability, percentile 0.541140000 (date 2026-04-12)

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	Stylemix	Pearl Header Builder	affected 1.3.6 semver	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/c23bba83-35d2-4098-8104-8389b...	af854a3a-2127-422b-91ae-364da2661108	www.wo
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	plugins.
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

CNA: Krzysztof Zając (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-04-30T00:00:00.000Z	Disclosed

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