ColorMag <= 3.1.6 - Authenticated (Contributor+) Stored Cross-Site Scripting via Display Name

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

Summary

CVE	CVE-2024-2500
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-22 02:15:09 UTC
Updated	2026-04-08 19:21:08 UTC
Description	The ColorMag theme for WordPress is vulnerable to Stored Cross-Site Scripting via a user's Display Name in all versions u

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: 0.002890000 probability, percentile 0.523970000 (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

ntegrity

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	Themegrill	ColorMag	affected 3.1.6 semver	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/a4b44d89-6f1e-4a23-91ea-e79fc...	af854a3a-2127-422b-91ae-364da2661108	www.wor
themes.trac.wordpress.org/browser/colormag/3.1.6/inc/template-tags.php	af854a3a-2127-422b-91ae-364da2661108	themes.tr
themes.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	themes.tr
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Discovery Credit

CNA: Matthew Rollings (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-03-21T00:00:00.000Z	Disclosed

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