Unilevel MLM Plan <= 1.1.0 - Reflected Cross-Site Scripting via 'page'

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

Summary

CVE	CVE-2024-12324
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-01-07 05:15:18 UTC
Updated	2026-04-08 19:19:58 UTC
Description	The Unilevel MLM Plan plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all v

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from security@wordfence.com

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

EPSS: 0.019050000 probability, percentile 0.832560000 (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	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Letscms	Unilevel MLM Plan	affected 1.1.0 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset/3392120	security@wordfence.com	plugins.trac.wordpre
www.wordfence.com/threat-intel/vulnerabilities/id/fe71e2b9-ddd7-4d6d-97e5-5fad4...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/browser/unilevel-mlm-plan/trunk/includes/admin/settings/view/...	security@wordfence.com	plugins.trac.wordpre
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: vgo0 (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-01-06T15:43:18.000Z	Disclosed

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