Binary MLM Plan <= 5.0 - Authenticated (Subscriber+) Insecure Direct Object Reference

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

Summary

CVE	CVE-2025-11895
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-17 10:15:33 UTC
Updated	2026-04-08 19:23:06 UTC
Description	The Binary MLM Plan plugin for WordPress is vulnerable to insecure direct object reference in versions up to, and including

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from security@wordfence.com

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

EPSS: 0.000340000 probability, percentile 0.099030000 (date 2026-04-13)

Problem Types: CWE-639 | CWE-639 CWE-639 Authorization Bypass Through User-Controlled Key

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Letscms	Binary MLM Plan	affected 5.0 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/binary-mlm-plan/trunk/includes/bmp-hook-functions.php	security@wordfence.com	plugins.trac.wordpre
www.wordfence.com/threat-intel/vulnerabilities/id/adba7d0c-29ca-49c5-ac75-bb79d...	security@wordfence.com	www.wordfence.cor
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Jonas Benjamin Friedli (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-10-16T20:57:56.000Z	Disclosed

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