Binary MLM Plan <= 3.0 - Unauthenticated Limited Privilege Escalation

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

Summary

CVE	CVE-2025-10038
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-10-15 09:15:36 UTC
Updated	2026-04-08 18:23:06 UTC
Description	The Binary MLM Plan plugin for WordPress is vulnerable to limited Privilege Escalation in all versions up to, and including,

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from security@wordfence.com

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

EPSS: 0.001130000 probability, percentile 0.299410000 (date 2026-04-08)

Problem Types: CWE-266 | CWE-266 CWE-266 Incorrect Privilege Assignment

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Letscms	Binary MLM Plan	affected 3.0 semver	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/7951c8e4-b610-4cc4-ab27-4cfa7...	security@wordfence.com	www.wordfence.
plugins.trac.wordpress.org/changeset/3380455/binary-mlm-plan/tags/5.0/includes/bmp-hook-...	security@wordfence.com	plugins.trac.word
wordpress.org/plugins/binary-mlm-plan	security@wordfence.com	wordpress.org
plugins.trac.wordpress.org/changeset/3380455/binary-mlm-plan/tags/5.0/includes/admin/cla...	security@wordfence.com	plugins.trac.word
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	2025-10-14T20:04:50.000Z	Disclosed

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