CRM Memberships <= 2.6 - Missing Authorization to Privilege Escalation via Unauthenticated Password Reset in 'ntzcrm_changepassword' AJAX Endpoint

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

Summary

CVE	CVE-2025-13313
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-05 05:16:57 UTC
Updated	2026-04-08 19:23:22 UTC
Description	The CRM Memberships plugin for WordPress is vulnerable to privilege escalation via password reset in all versions up to, a

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from security@wordfence.com

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

EPSS: 0.003380000 probability, percentile 0.566520000 (date 2026-04-13)

Problem Types: CWE-862 | CWE-862 CWE-862 Missing Authorization

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Dripadmin	CRM Memberships	affected 2.6 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/crm-memberships/tags/2.5/ntzcrm-memberships.php	security@wordfence.com	plugins.trac.wordp
plugins.trac.wordpress.org/changeset/3464130	security@wordfence.com	plugins.trac.wordp
plugins.trac.wordpress.org/browser/crm-memberships/tags/2.5/includes/class/class-ntzcrm-...	security@wordfence.com	plugins.trac.wordp
plugins.trac.wordpress.org/browser/crm-memberships/tags/2.5/includes/class/class-ntzcrm-...	security@wordfence.com	plugins.trac.wordp
www.wordfence.com/threat-intel/vulnerabilities/id/e2837399-c44f-494e-bdc6-f9c6e...	security@wordfence.com	www.wordfence.c
plugins.trac.wordpress.org/browser/crm-memberships/tags/2.5/includes/class/class-ntzcrm-...	security@wordfence.com	plugins.trac.wordp
plugins.trac.wordpress.org/browser/crm-memberships/tags/2.5/includes/class/class-ntzcrm-...	security@wordfence.com	plugins.trac.wordp
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Athiwat Tiprasaharn (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-12-04T16:27:00.000Z	Disclosed

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report