REST API TO MiniProgram <= 4.7.1 - Unauthenticated Arbitrary User Email Update and Privilege Escalation via Account Takeover

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

Summary

CVE	CVE-2024-8485
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-09-25 03:15:05 UTC
Updated	2026-04-08 19:22:25 UTC
Description	The REST API TO MiniProgram plugin for WordPress is vulnerable to privilege escalation via account takeovr in all version

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: 0.003580000 probability, percentile 0.580150000 (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	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

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jianbo	Rest Api To Miniprogram	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Xjb	REST API TO MiniProgram	affected 4.7.1 semver	Not specified
ADP	Jianbo	Rest-api-to-miniprogram	affected 4.7.1 custom	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/b53066d3-2ff3-4460-896a-facd7...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/browser/rest-api-to-miniprogram/tags/4.7.0/includes/api/ram-r...	security@wordfence.com	plugins.trac.wordpres
plugins.trac.wordpress.org/browser/rest-api-to-miniprogram/tags/4.7.6/includes/api/ram-r...	security@wordfence.com	plugins.trac.wordpres
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: wesley (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-09-24T12:22:54.000Z	Disclosed

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