



LadiApp <= 4.4 - Missing Authorization via save_config()

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2023-4627
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-12 10:15:07 UTC
Updated	2026-04-08 19:18:32 UTC
Description	The LadiApp plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on th

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:N/I:L/A:N

EPSS: 0.001070000 probability, percentile 0.289540000 (date 2026-04-12)

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

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:N/I:L/A:N
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ladipage	Ladipage	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Binhnguyenplus	LadiApp Landing Page PopupX Marketing Automation Affiliate Marketing	affected 4.4 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/ladipage/trunk/ladipage.php	af854a3a-2127-422b-91ae-364da2661108	plugins.trac.wordpress.org
www.wordfence.com/threat-intel/vulnerabilities/id/d8074af6-cb2c-44db-9110-517f3...	af854a3a-2127-422b-91ae-364da2661108	www.wordfence.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: GiongNef (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-03-11T00:00:00.000Z	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