LadiApp <= 4.4 - Cross-Site Request Forgery via ladiflow_save_hook()

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

Summary

CVE	CVE-2023-4628
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 17:17:03 UTC
Description	The LadiApp plugin for WordPress is vulnerable to Cross-Site Request Forgery due to a missing nonce check on the ladiflo

Risk And Classification

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

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

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/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
www.wordfence.com/threat-intel/vulnerabilities/id/0be418fa-f1cf-4aaf-bc94-c8e04...	af854a3a-2127-422b-91ae-364da2661108	www.wordf
plugins.trac.wordpress.org/browser/ladipage/trunk/ladipage.php	af854a3a-2127-422b-91ae-364da2661108	plugins.trac
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

Vendor Comments And Credit

Discovery Credit

CNA: GiongfNef (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.

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