WordPress WP Optin Wheel Plugin <= 1.4.3 is vulnerable to Sensitive Data Exposure

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

Summary

CVE	CVE-2023-51408
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-01-08 21:15:09 UTC
Updated	2026-04-28 19:22:44 UTC
Description	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in StudioWombat WP Optin Wheel – Gamified Opt

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

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

EPSS: 0.006930000 probability, percentile 0.719140000 (date 2026-04-28)

Problem Types: CWE-532 | CWE-532 CWE-532 Insertion of Sensitive Information into Log File

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Studiowombat	Wp Optin Wheel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	StudioWombat	WP Optin Wheel Gamified Optin Email Marketing Tool For WordPress And WooCommerce	affected n/a 1.4.3 cu

References

Reference	Source	Link
patchstack.com/database/vulnerability/wp-optin-wheel/wordpress-wp-optin-whee...	af854a3a-2127-422b-91ae-364da2661108	patchstack.
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

Vendor Comments And Credit

Discovery Credit

CNA: Joshua Chan (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 1.4.4 or a higher version.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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