WP-Eggdrop <= 0.1 - Authenticated (Admin+) Stored Cross-Site Scripting

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

Summary

CVE	CVE-2024-2968
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-29 07:15:46 UTC
Updated	2026-04-08 17:18:39 UTC
Description	The WP-Eggdrop plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to,

Risk And Classification

Primary CVSS: v3.1 4.8 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-79 | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
3.1	security@wordfence.com	Secondary	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	4.4	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Backie	Wp-eggdrop	0.1	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Backie	WP-Eggdrop	affected 0.1 semver	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/21238925-b87c-43ea-b4ab-9b5d3...	af854a3a-2127-422b-91ae-364da2661108	www.wo
plugins.trac.wordpress.org/browser/wp-eggdrop/trunk/wp-eggdrop.php	af854a3a-2127-422b-91ae-364da2661108	plugins.
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

CNA: Benedictus Jovan (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-03-28T00:00:00.000Z	Disclosed

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

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