WP-Eggdrop <= 0.1 - Cross-Site Request Forgery to Settings Update

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

Summary

CVE	CVE-2024-2969
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 Cross-Site Request Forgery in all versions up to, and including, 0.1.

Risk And Classification

Primary CVSS: v3.1 5.4 MEDIUM from security@wordfence.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/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	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
Low

Privileges Required
None

User Interaction
Required

Scope
Unchanged

Confidentiality
Low

Integrity
Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/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
plugins.trac.wordpress.org/browser/wp-eggdrop/trunk/wp-eggdrop.php	af854a3a-2127-422b-91ae-364da2661108	plugins.tr
www.wordfence.com/threat-intel/vulnerabilities/id/2cd509f7-100a-4f28-8d5a-b6b90...	af854a3a-2127-422b-91ae-364da2661108	www.wor
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

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.

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