Splitit <= 4.2.8 - Missing Authorization to Multiple Administrative Actions

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

Summary

CVE	CVE-2025-4105
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-21 12:16:22 UTC
Updated	2026-04-08 18:24:46 UTC
Description	The Splitit plugin for WordPress is vulnerable to unauthorized modification of data due to missing capability checks on seve

Risk And Classification

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

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

EPSS: 0.001590000 probability, percentile 0.367610000 (date 2026-04-08)

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

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

Low

vailability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Splitit	Splitit	affected 4.2.8 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.trac.wordpress.or
plugins.trac.wordpress.org/browser/splitit-installment-payments/tags/4.2.6/splitIt-flexf...	security@wordfence.com	plugins.trac.wordpress.or
www.wordfence.com/threat-intel/vulnerabilities/id/6471b075-8115-4d38-a7dd-2308d...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/browser/splitit-installment-payments/tags/4.2.6/splitIt-flexf...	security@wordfence.com	plugins.trac.wordpress.or
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Sushi Com Abacate (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-05-20T20:31:09.000Z	Disclosed

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