Relevanssi <= 4.24.4 (Free) and <= 2.27.5 (Premium) - Unauthenticated SQL Injection

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

Summary

CVE	CVE-2025-4396
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-13 04:16:27 UTC
Updated	2026-04-08 17:20:44 UTC
Description	The Relevanssi – A Better Search plugin for WordPress is vulnerable to time-based SQL Injection via the cats and tags que

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from security@wordfence.com

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

Problem Types: CWE-89 | CWE-89 CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/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

Integrity

None

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Relevanssi	Relevanssi Premium	affected 2.27.5 semver	Not specified
CNA	Comesio	Relevanssi A Better Search	affected 4.24.4 semver	Not specified

References

Reference	Source	Link
plugins.trac.wordpress.org/browser/relevanssi/tags/4.24.4/lib/search-tax-query.php	security@wordfence.com	plugins.trac.wordpress.or
plugins.trac.wordpress.org/browser/relevanssi/tags/4.24.4/lib/search.php	security@wordfence.com	plugins.trac.wordpress.or
plugins.trac.wordpress.org/browser/relevanssi/tags/4.24.4/lib/search.php	security@wordfence.com	plugins.trac.wordpress.or
www.wordfence.com/threat-intel/vulnerabilities/id/197be163-4504-4caa-b729-c3293...	security@wordfence.com	www.wordfence.com
plugins.trac.wordpress.org/browser/relevanssi/tags/4.24.4/lib/search-tax-query.php	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: Jack Taylor (en)

Additional Advisory Data

Source	Time	Event
CNA	2025-05-03T00:00:00.000Z	Discovered
CNA	2025-05-12T14:38:29.000Z	Disclosed

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

Free CVE JSON API cve.report/api

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