Country State City Dropdown CF7 <= 2.7.2 - Unauthenticated SQL Injection

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

Summary

CVE	CVE-2024-3495
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-05-22 09:15:12 UTC
Updated	2026-04-08 17:18:42 UTC
Description	The Country State City Dropdown CF7 plugin for WordPress is vulnerable to SQL Injection via the ‘cnt’ and 'sid' parameters

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from security@wordfence.com

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

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	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Trustyplugins	Country State City Dropdown CF7	affected 2.7.2 semver	Not specified

References

Reference	Source	Lir
plugins.trac.wordpress.org/browser/country-state-city-auto-dropdown/trunk/includes/ajax-...	af854a3a-2127-422b-91ae-364da2661108	plu
plugins.trac.wordpress.org/browser/country-state-city-auto-dropdown/trunk/includes/ajax-...	af854a3a-2127-422b-91ae-364da2661108	plu
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	plu
www.wordfence.com/threat-intel/vulnerabilities/id/17dcacaf-0e2a-4bef-b944-fb7e4...	af854a3a-2127-422b-91ae-364da2661108	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

Vendor Comments And Credit

Discovery Credit

CNA: Krzysztof Zając (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-05-21T19:38:42.000Z	Disclosed

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