



WordPress WP Travel Engine plugin <= 5.7.9 - SQL Injection vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2024-30504
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-29 15:15:13 UTC
Updated	2026-04-28 19:24:06 UTC
Description	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP Travel Engine.

Risk And Classification

Primary CVSS: v3.1 7.2 HIGH from nvd@nist.gov

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

EPSS: 0.005560000 probability, percentile 0.682110000 (date 2026-04-28)

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	nvd@nist.gov	Primary	7.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	audit@patchstack.com	Secondary	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:L
3.1	CNA	CVSS	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wptravelengine	Wp Travel Engine	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	WP Travel Engine	WP Travel Engine	affected n/a 5.7.9 custom	Not specified
ADP	Wptravelengine	Wp Travel Engine	affected 5.7.9 custom	Not specified

References

Reference	Source	Link
WordPress WP Travel Engine plugin <= 5.7.9 - SQL Injection vulnerability - Patchstack	af854a3a-2127-422b-91ae-364da2661108	patches
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

Vendor Comments And Credit

Discovery Credit

CNA: Yudistira Arya (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 5.8.0 or a higher version.

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

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web 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