‹ To plugin page

Not fixed

WordPress Travel Management plugin <= 2.0 - Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities

4.1

CVSS 3.1 score

Medium severity

Report

Monitoring

Not reported to be exploited

Software	Travel Management

Type	Plugin
Vulnerable versions	<= 2.0
Fixed in	N/A
PSID	ae2a8b39a3d3
CVE ID	CVE-2022-27859
Classification	Cross Site Scripting (XSS)
OWASP Top 10	A7: Cross-Site Scripting (XSS)
Required privilege	Requires contributor or higher role user authentication.
Credits	Ngo Van Thien (Alliance project)
Publicly disclosed	2022-05-26

Details

Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities were discovered by Ngo Van Thien (Patchstack Alliance) in the WordPress Travel Management plugin (versions <= 2.0).

Solution

Deactivate and delete. This plugin has been closed as of May 6, 2022 and is not available for download. This closure is temporary, pending a full review.

References

CVE-2022-27859

Plugin page

Other known vulnerabilities for Travel Management

Unauthenticated Options Change vulnerability	<= 1.5

Submit vulnerabilities and become a verified Alliance member

Learn more >

WordPress security

Plugin auditing

Vulnerability database

Vulnerability API

Bug bounty program BETA

Patchstack for WordPress

For agencies NEW

Pricing & features

Documentation

Changelog

About us

Careers

Media kit

Insights & articles