



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in WordPress plugin

Tracking #:432316337

Date:27-09-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical SQL Injection vulnerability in The Events Calendar plugin for WordPress.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-8275**
- **CVSS Score:** 9.8 (**Critical**)
- The Events Calendar plugin for WordPress, up to version 6.6.4, has been identified as vulnerable to SQL Injection attacks. This vulnerability arises from the 'order' parameter of the tribe_has_next_event function, which lacks adequate escaping for user-supplied input and does not sufficiently prepare the SQL query.
- As a result, unauthenticated attackers can inject additional SQL queries into existing ones, potentially allowing them to extract sensitive information from the database.

Affected Versions:

- All versions up to and including 6.6.4

Fixed Versions:

- Version 6.6.4.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the affected versions to the latest version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/the-events-calendar/the-events-calendar-664-unauthenticated-sql-injection>