مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Ultimate Member WordPress plugin

Tracking #:432315654

Date:27-02-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the Ultimate Member WordPress plugin that could be exploited by attackers to gain unauthorized access and obtain sensitive information from affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-1071**
- CVSS score 9.8 Critical
- A critical SQL Injection (SQLi) vulnerability in the Ultimate Member WordPress plugin. This vulnerability allows unauthenticated attackers to inject additional SQL queries and potentially extract sensitive data from the database. The vulnerability arises from insufficient escaping on the 'sorting' parameter and inadequate preparation on the existing SQL query.
  - Unauthenticated attackers can exploit this vulnerability to compromise websites that have enabled the "Enable custom table for usermeta" option in the plugin settings.
  - Attackers could append malicious SQL queries to gain unauthorized access and extract sensitive information from the database.

Affected Versions:

- 2.1.3 - 2.8.2

Fixed Versions:

- 2.8.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Vendor.

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:

1.https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/ultimate-member/ultimate-member-user-profile-registration-login-member-directory-content-restriction-membership-plugin-213-282-unauthenticated-sql-injection