مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities Patched in WPLMS and VibeBP Plugins

Tracking #:432316671

Date:25-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security has observed multiple critical vulnerabilities in the WPLMS WordPress theme and its associated VibeBP plugin. These vulnerabilities pose significant risks to website security and data integrity.

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been identified and patched in the WPLMS WordPress theme and its associated VibeBP plugin. These vulnerabilities pose significant risks, including unauthorized file uploads, privilege escalation, and SQL injection attacks.

WPLMS Theme Vulnerabilities:

1. CVE-2024-56046 (CVSS 10.0): Allows unauthenticated attackers to upload malicious files, potentially leading to remote code execution (RCE)
2. CVE-2024-56050 (CVSS 9.9): Authenticated users with subscriber privileges can bypass restrictions to upload files
3. CVE-2024-56052 (CVSS 9.9): Similar to CVE-2024-56050 but exploitable by users with student roles
4. CVE-2024-56043 (CVSS 9.8): Enables attackers to register as any role, including Administrator, without authentication
5. CVE-2024-56048 (CVSS 8.8): Allows low-privilege users to escalate to higher roles, such as Administrator, by exploiting weak role validation
6. CVE-2024-56042 (CVSS 9.3): Permits attackers to inject malicious SQL queries to extract sensitive data or compromise the database
7. CVE-2024-56047 (CVSS 8.5): Enables low-privilege users to execute SQL queries, potentially compromising data integrity or confidentiality

.

VibeBP Plugin Vulnerabilities:

1. CVE-2024-56040 (CVSS 9.8): Allows attackers to register as privileged users without authentication
2. CVE-2024-56039 (CVSS 9.3): Enables unauthenticated users to inject SQL queries by exploiting poorly sanitized inputs
3. CVE-2024-56041 (CVSS 8.5): Permits authenticated users with minimal privileges to perform SQL injection to compromise or extract database information

Affected Versions:

- **WPLMS Theme**: Versions prior to **1.9.9.5.3**.
- **VibeBP Plugin**: Versions prior to **1.9.9.7.7**.

Fixed Versions:

- **WPLMS 1.9.9.5.3** or later.
- **VibeBP 1.9.9.7.7** or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://patchstack.com/articles/multiple-critical-vulnerabilities-patched-in-wplms-and-vibebp-plugins/