مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in WordPress LiteSpeed Cache Plugin

Tracking #:432316176
Date:23-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in WordPress LiteSpeed Cache Plugin that could be exploited to gain unauthorized access to vulnerable websites.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-28000**
- **Severity:** **Critical** (CVSS score: 9.8)
- A critical vulnerability exists in the LiteSpeed Cache plugin for WordPress that could allow unauthenticated attackers to gain administrator-level access to vulnerable websites.
- The vulnerability stems from a flaw in the plugin's user simulation feature. An unauthenticated attacker can exploit this flaw to spoof their user ID and register as an administrator-level user, effectively gaining control of the WordPress site.
- **Impact:** Unrestricted access to the WordPress site, including the ability to upload and install malicious plugins.

Affected Versions:

- All versions of LiteSpeed Cache prior to 6.4

Fixed Versions:

- LiteSpeed Cache version **6.4** or later

RECOMMENDATIONS:

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

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://nvd.nist.gov/vuln/detail/CVE-2024-28000