مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in LiteSpeed Cache WordPress Plugin

Tracking #:432316462
Date:01-11-2024

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

- **CVE-2024-50550**
- CVSS Score: 8.1 (High)
- A high-severity vulnerability exists in LiteSpeed Cache WordPress plugin, affecting over 6 million active installations. This unauthenticated privilege escalation flaw allows attackers to potentially gain Administrator access to vulnerable WordPress sites.
- The vulnerability exploits a weakness in the plugin's user simulation feature, which uses a weak security hash check with known values. By manipulating the Crawler settings and exploiting the flawed hash generation process, an attacker can bypass security checks and gain unauthorized administrative access.
- Successful exploitation could allow an attacker to:
    - Gain unauthorized Administrator-level access to WordPress sites
    - Upload and activate malicious plugins
    - Compromise the security and integrity of affected websites

Affected Versions

- LiteSpeed Cache versions prior to 6.5.2

Fixed Versions:

- LiteSpeed Cache version 6.5.2 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/rare-case-of-privilege-escalation-patched-in-litespeed-cache-plugin/
- https://nvd.nist.gov/vuln/detail/CVE-2024-50550