مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

LiteSpeed Cache Vulnerability Exploited for WordPress Admin Takeover

Tracking #:432315838

Date:09-05-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed threat actors actively exploiting a High-Severity vulnerability in the LiteSpeed Cache plugin for WordPress. This vulnerability allows attackers to inject malicious code into websites, potentially compromising user data and website functionality.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2023-40000) in the LiteSpeed Cache plugin for WordPress is under active exploitation. Hackers are using this flaw to create unauthorized administrator accounts on vulnerable websites. This compromise grants them full control over the site, allowing them to inject malware, steal data, or redirect visitors to malicious pages.

Vulnerability Details:

- **CVE-2023-40000**
- **CVSS Score:** 8.3 (High Severity)
- The vulnerability is a stored XSS (Cross-Site Scripting) flaw that arises due to improper user input validation.
- An attacker can exploit this vulnerability to gain full control over a vulnerable WordPress website. This could include injecting malware, installing malicious plugins, stealing sensitive information, or redirecting users to fraudulent websites.

Indicators of Compromise (IoCs):

- Presence of new administrator accounts named "wpsupp-user" or "wp-configuser".
- Suspicious JavaScript code injected into WordPress files.
- Malicious code referencing domains like "dns.startservicefounds[.]com" and "api.startservicefounds[.]com".
- Presence of the string "eval(atob(Strings.fromCharCode'" in the WordPress database option "litespeed.admin_display.messages".

Affected Versions:
LiteSpeed Cache plugin for WordPress versions prior to 5.7.0.1

Latest Version:
LiteSpeed Cache plugin for WordPress version 6.2.0.1

RECOMMENDATIONS:

- Update the LiteSpeed Cache plugin to the latest version
- **Change Passwords:** Change the passwords for all administrator accounts on website. Use strong, unique passwords for each account.
- **Scan for Malicious Code:** Scan website files and database for signs of compromise, such as injected code or suspicious files.
- **Review Admin Accounts:** Check WordPress user accounts and delete any unrecognized or suspicious accounts.
- **Maintain Backups:** Regularly back up website data to facilitate a swift recovery in case of an attack.

- **Monitor Activity:** Closely monitor website logs for any suspicious activity after patching the vulnerability.

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://wpscan.com/blog/surge-of-javascript-malware-in-sites-with-vulnerable-versions-of-litespeed-cache-plugin/
- https://patchstack.com/database/vulnerability/litespeed-cache/wordpress-litespeed-cache-plugin-5-7-unauthenticated-site-wide-stored-xss-vulnerability?_s_id=cve