مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in LiteSpeed Cache Plugin for WordPress

Tracking #:432316229
Date:06-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the LiteSpeed Cache plugin for WordPress that could potentially be exploited to gain control over affected websites.

TECHNICAL DETAILS:

A critical security vulnerability exists in the LiteSpeed Cache plugin for WordPress, which has over 5 million active installations. This flaw allows unauthenticated visitors to hijack logged-in user accounts, including those with administrator privileges, posing a significant threat to WordPress users.

Vulnerability Details:

- **CVE-2024-44000**
- **CVSS Score:** 9.8 (Critical)
- The vulnerability stems from a flaw in the plugin's debug log feature, which inadvertently leaks HTTP response headers, including sensitive "Set-Cookie" headers. This allows attackers to hijack user sessions and potentially gain access to administrator accounts.
- **Conditions for Exploitation**
  - The debug log feature must be active or have been previously activated without the log file being purged.
  - The attacker must be able to access the /wp-content/debug.log file.

Impact:

Successful exploitation of this vulnerability could grant attackers complete control over the affected website, allowing them to hijack user sessions, gain unauthorized access to sensitive data, and upload and execute malicious code.

Fixed Version:

- LiteSpeed Cache version 6.5.0.1 or later

RECOMMENDATIONS:

- **Update Plugin:** Immediately update LiteSpeed Cache to version 6.5.0.1 or later.
- **Review Security Rules:** Ensure that your .htaccess settings restrict access to log files effectively.
- **Purge Logs:** Clear the debug.log file if it has ever been enabled, to protect against cookie leakage.
- **Monitor Access:** Continuously monitor for unauthorized access attempts and unusual activity on your WordPress site.

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/critical-account-takeover-vulnerability-patched-in-litespeed-cache-plugin/