NCSC
National Cyber Security Centre

2408220138-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerability exists in LiteSpeed Technologies LiteSpeed Cache Wordpress Plugin (CVE-2024-28000, CVSSv3: 9.8)

Thursday 22nd August, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.*

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.
Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-08-21 14:15:00
Vendor: LiteSpeed Technologies
Product: LiteSpeed Cache
CVE ID: CVE-2024-28000
CVSS3.0 Score[1]**:** 9.8
EPSS[2]**:** 0.095360000
For up to date EPSS score, click here: https://api.first.org/data/v1/epss?cve=CVE-2024-28000
Summary:
Incorrect Privilege Assignment vulnerability in LiteSpeed Technologies LiteSpeed Cache litespeed-cache allows Privilege Escalation in the popular Wordpress plugin.

Products Affected

LiteSpeed Technologies LiteSpeed Cache

- All versions 1.9 <= 6.3.0.1

Impact

Common Weakness Enumeration (CWE)[3]**:** CWE-266 Incorrect Privilege Assignment
Present in CISA Known Exploited Vulnerability(KEV)[4] **catalog:** NO
Used by Ransomware Operators: Not Known

Recommendations

The NCSC strongly advises affected organisations to review their Wordpress configurations and review the latest release notes and install version 6.4 of the LiteSpeed Cache and any other the relevant updates.

Additional information can be found in the link(s) below:

- Patch Release Notes: https://wordpress.org/plugins/litespeed-cache/#developers
- Vulnerability summary: https://patchstack.com/database/vulnerability/litespeed-cache/wordpress-litespeed-cache-plugin-6-3-0-1-unauthenticated-privilege-escalation-vulnerability?_s_id=cve
- Vulnerability details: https://patchstack.com/articles/critical-privilege-escalation-in-litespeed-cache-plugin-affecting-5-million-sites?_s_id=cve

[1] https://www.first.org/cvss/v3.0/specification-document
[2] https://www.first.org/epss/articles/prob_percentile_bins
[3] https://cwe.mitre.org/
[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta
Cibearshlándála
National Cyber Security Centre