

CVE-2026-48172

LiteSpeed cPanel Plugin Privilege Escalation Vulnerability

CISA KEV since May 26, 2026

Actively exploited

LiteSpeed User-End cPanel Plugin before 2.4.5 allows privilege escalation (possibly to root), as exploited in the wild in May 2026. Detection is best done via a command line of `grep -rE "cpanel_jsonapi_func=redisAble" /var/cpanel/logs /usr/local/cpanel/logs/ 2>/dev/null` in Bash. If you get no output, you have not been hit with exploitation of the vulnerability. If there is output, we recommend you examine the IP addresses in the list, determine if they are valid IP addresses, and if not, block them.

EVRS 75/₁₀₀ Urgent priority	CVSS V4.0 10.0 Critical · NVD	EPSS 0.010 62.8th percentile · FIRST	CISA DEADLINE May 29, 2026 CISA federal deadline · Overdue by 5 months
---	---	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.010 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

To determine damage done, examine the system logs for use by the detected IP addresses. The issue is related to mishandling of Redis enable/disable features. The recommended minimum version is 2.4.7.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
litespeed cpanel plugin	< 2.4.7	2.4.7	NVD
litespeed whm plugin	< 5.3.1.0	5.3.1.0	NVD

Sources

Vendor guidance github.com/advisories/GHSA-fxrh-cwjh-m33v

Additional guidance blog.litespeedtech.com/2026/05/21/security-update-for-litespeed-cpanel-plugin/

NVD nvd.nist.gov/vuln/detail/CVE-2026-48172

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2026-31204

Current data evulnable.com/vulnerability-management/cve/CVE-2026-48172

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.