



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Actively Exploited Critical Vulnerability in LiteSpeed User-End cPanel Plugin**  
Tracking #:432319022  
Date:25-05-2026

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical privilege escalation vulnerability in the LiteSpeed user-end plugin for cPanel. The vulnerability is actively being exploited in the wild and may allow authenticated cPanel users to execute arbitrary scripts with root privileges.

## TECHNICAL DETAILS:

### Vulnerability Details

- **CVE-2026-48172**
- **Severity:** Critical | **CVSS:** 10.0
- A privilege escalation vulnerability exists in the LiteSpeed user-end plugin for cPanel due to improper handling of the `lsws.redisAble` function. An authenticated cPanel user, including a compromised account, may exploit this flaw to execute arbitrary scripts as the root user. Successful exploitation could result in full system compromise.

### Affected Versions

- LiteSpeed User-End cPanel Plugin versions v2.3 through v2.4.4

### Fixed Versions

- LiteSpeed WHM Plugin v5.3.1.0 (bundled w/ cPanel plugin v2.4.7) or later.

### Indicators of Compromise (IOC)

To check for potential exploitation: Run the following command in Bash

```
grep -rE "cpanel_jsonapi_func=redisAble" /var/cpanel/logs /usr/local/cpanel/logs/ 2>/dev/null
```

- No output indicates no detected exploitation attempts.
- Any output should be reviewed to identify suspicious or unauthorized IP addresses.

## RECOMMENDATIONS:

- Immediately update affected LiteSpeed cPanel plugins to the latest available version.
- Review server and cPanel logs for suspicious activity or unauthorized access attempts.
- Investigate and block untrusted IP addresses identified in exploitation attempts.
- Monitor systems for indicators of compromise and unauthorized privilege escalation activities.
- Ensure all LiteSpeed and cPanel components are regularly updated with the latest security patches.

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://www.cve.org/CVERecord?id=CVE-2026-48172>