مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in LiteSpeed cPanel Plugin

Tracking #:432319141

Date:16-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a privilege escalation vulnerability in the LiteSpeed cPanel User-End Plugin. The flaw allows attackers with FTP or web shell access to escalate privileges to root on shared hosting environments using CloudLinux/CageFS. The vulnerability is actively being exploited in the wild, posing a severe risk to affected hosting infrastructures.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-54420**
- **Severity:** High **| CVSS:** 8.5
- The vulnerability exists in the LiteSpeed cPanel plugin when processing symbolic links created or manipulated by users with limited access (e.g., FTP users or web shell-compromised accounts). Due to improper symlink validation, attackers can potentially trick the plugin into following unauthorized symbolic links, enabling access to restricted files or escalation of privileges within shared hosting environments.
- This issue primarily impacts systems using shared hosting isolation mechanisms such as CloudLinux and CageFS, where symlink restrictions are expected to enforce tenant separation.
- LiteSpeed has confirmed that exploitation of this vulnerability has been observed in the wild.

Affected Products and Versions

- LiteSpeed cPanel User-End Plugin versions prior to 2.4.8
- Shared hosting servers running CloudLinux/CageFS
- LiteSpeed WHM Plugin is not affected, but older bundled user-end plugin versions remain vulnerable

Fixed Versions

- LiteSpeed cPanel Plugin v2.4.8 or later
- LiteSpeed WHM Plugin v5.3.2.1 or later

Indicators of Compromise (IoCs)

Detection Command:

```
grep -rE 'cpanel_jsonapi_func=(generateEcCert|packageUserSize)|cert_action_entry .*geneccert' /usr/local/cpanel/logs/ /var/cpanel/logs/ 2>/dev/null
```

Potential indicators include:

- generateEcCert immediately followed by packageUserSize for the same user
- Multiple concurrent requests (typically 7–10) during an exploitation attempt
- The same source IP repeatedly accessing both endpoints

RECOMMENDATIONS:

- Immediately upgrade all affected LiteSpeed plugins to patched versions
- Review cPanel and system logs for signs of exploitation.
- Investigate suspicious IP addresses associated with identified events.
- Monitor systems for unauthorized privilege escalation and post-exploitation activity.
- Enable automatic updates where operationally feasible.

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://blog.litespeedtech.com/2026/06/01/security-update-for-litespeed-cpanel-plugin-2/
- https://www.tenable.com/cve/CVE-2026-54420