DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 24-05-2026

BULLETIN ALERTES

Object	Vulnérabilité Critique dans le Plugin LiteSpeed pour cPanel
Réference	1480
Date de Publication	2026-05-24
Sévérité	Critique

IMPACT :

- Élévation de privilèges jusqu'au niveau **root**
- Exécution de scripts arbitraires sur le serveur
- Compromission complète du serveur d'hébergement
- Mouvement latéral dans les environnements d'hébergement mutualisé

SYSTÉME AFFECTÉ :

- La vulnérabilité affecte tous les serveurs cPanel exécutant le **LiteSpeed User-End cPanel Plugin** dans les versions comprises entre **2.3** et **2.4.4** (incluses).
- Le plugin WHM de LiteSpeed n'est **pas impacté**.

DÉSCRIPTION :

Une vulnérabilité de sévérité maximale a été découverte dans le plugin LiteSpeed User-End pour cPanel, identifiée comme **CVE-2026-48172** (score CVSS : 10.0). La faille résulte d'une attribution incorrecte de privilèges au sein de la fonction lsws.redisAble. Tout utilisateur cPanel — y compris un attaquant disposant d'un compte ordinaire ou d'un compte compromis — peut exploiter cette fonction pour exécuter des scripts arbitraires avec les droits **root** sur le serveur. Aucune interaction supplémentaire de la victime n'est requise une fois le compte compromis.

SOLUTION :

Consulter le bulletin de sécurité de l’éditeur afin d’obtenir les correctifs (cf. section Documentation).

DOCUMENTATION :

- CVE-2026-48172 (NVD) :

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

- Bulletin officiel LiteSpeed :

https://blog.litespeedtech.com/2026/05/21/security-update-for-litespeed-cpanel-plugin/