Una vulnerabilidad de seguridad de máxima gravedad que afecta al complemento LiteSpeed User-End para cPanel está siendo explotada activamente en entornos reales.

La falla, identificada como CVE-2026-48172 (puntaje CVSS: 10.0), está relacionada con una asignación incorrecta de privilegios que podría ser aprovechada por un atacante para ejecutar scripts arbitrarios con permisos elevados.

«Cualquier usuario de cPanel (incluyendo un atacante o una cuenta comprometida) puede explotar la función lsws.redisAble para ejecutar scripts arbitrarios como root», indicó LiteSpeed.

La vulnerabilidad afecta a todas las versiones del complemento comprendidas entre la 2.3 y la 2.4.4. El complemento WHM de LiteSpeed no se ve afectado. El problema fue corregido en la versión 2.4.5. El investigador de seguridad David Strydom fue reconocido por descubrir y reportar la falla.

LiteSpeed señaló que *"la vulnerabilidad está siendo explotada activamente"*, aunque evitó proporcionar más detalles técnicos. No obstante, publicó el siguiente indicador de compromiso:

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

Si al ejecutar el comando "grep" mencionado anteriormente no se obtiene ninguna salida, el servidor no está comprometido. Sin embargo, si aparece algún resultado, se recomienda revisar las direcciones IP listadas para verificar si son legítimas y, en caso contrario, bloquearlas.

Tras una revisión de seguridad de sus complementos para cPanel y WHM a raíz de esta

vulnerabilidad, LiteSpeed informó que corrigió otros posibles vectores de ataque en ambos plugins y publicó la versión 2.4.7 del complemento de cPanel como parte de la versión 5.3.1.0 del plugin WHM.

Se recomienda a los usuarios actualizar a LiteSpeed WHM Plugin versión 5.3.1.0, que incluye el complemento cPanel v2.4.7 o superior, para mitigar la vulnerabilidad. Si no es posible aplicar el parche de inmediato, se aconseja eliminar el complemento del lado del usuario ejecutando el siguiente comando:

```
/usr/local/lsws/admin/misc/lscmctl cpanelplugin --uninstall
```

Este incidente ocurre semanas después de que otra vulnerabilidad crítica de cPanel (CVE-2026-41940, puntaje CVSS: 9.8) fuera identificada como explotada activamente por actores de amenazas desconocidos para desplegar variantes de la botnet Mirai y una familia de ransomware llamada Sorry.