TIC

ALERTA

Riesgo para millones de sitios WordPress

COLCERT AL-0410-051

Una reciente investigación de seguridad ha revelado una grave vulnerabilidad en el popular plugin de WordPress, **LiteSpeed Cache.** Esta falla de seguridad, catalogada como **CVE-2024-47374**, permite a los atacantes inyectar y ejecutar código JavaScript malicioso en sitios web que utilizan este plugin, poniendo en riesgo la seguridad de millones de sitios de WordPress en todo el mundo.

TLP:CLEAR

ELEMENTOS DE INTELIGENCIA DISPONIBLES

La vulnerabilidad es un tipo específico de ataque conocido como XSS almacenado, lo que significa que el código malicioso se almacena directamente en la base de datos del sitio web. Cada vez que un usuario visita una página afectada.

ANÁLISIS

El código malicioso se ejecuta automáticamente, lo que permite a los atacantes.

- **Robar información sensible:** Como contraseñas, cookies de sesión y otros datos personales.
- **Escalar privilegios:** Obtener acceso a áreas restringidas del sitio web, como el panel de administración.
- **Tomar el control completo del sitio:** Los atacantes pueden utilizar el sitio web comprometido para lanzar ataques a otros sitios o para difundir más malware.

IMPACTO PARA COLOMBIA Y LA REGIÓN

La vulnerabilidad CVE-2024-47374 en LiteSpeed Cache subraya la importancia de mantener actualizados los sitios de WordPress y de estar al tanto de las últimas amenazas de seguridad. Al tomar las medidas adecuadas, los propietarios de sitios web pueden proteger sus sitios y los datos de sus usuarios.

NIVEL DE RIESGO

MEDIO

FUENTES:

https://www.infosecurity-magazine.com/news/litespeed-cache-plugin-flaw-allows/
https://thehackernews.com/2024/10/wordpress-litespeed-cache-plugin.html

COLCERT