Investigadores en ciberseguridad han revelado una grave vulnerabilidad en el plugin LiteSpeed Cache para WordPress que podría permitir a usuarios no autenticados obtener privilegios de administrador.

> *«El plugin presenta una vulnerabilidad de escalada de privilegios no autenticada, lo que permite a cualquier visitante sin autenticación obtener acceso de nivel Administrador, permitiendo así la carga e instalación de plugins maliciosos,»* comentó Rafie Muhammad de Patchstack en un informe el miércoles.

La vulnerabilidad, catalogada como CVE-2024-28000 (puntuación CVSS: 9.8), fue solucionada en la versión 6.4 del plugin, lanzada el 13 de agosto de 2024. Afecta a todas las versiones del plugin, incluidas y anteriores a la 6.3.0.1.

LiteSpeed Cache es uno de los plugins de caché más populares en WordPress, con más de cinco millones de instalaciones activas.

En términos simples, CVE-2024-28000 permite a un atacante no autenticado suplantar su ID de usuario y registrarse como un usuario con nivel de administrador, otorgándole el control total sobre un sitio de WordPress vulnerable.

La vulnerabilidad se origina en una función de simulación de usuario dentro del plugin que utiliza un hash de seguridad débil, afectado por el uso de un número aleatorio fácilmente predecible como semilla.

En particular, solo hay un millón de combinaciones posibles para el hash de seguridad, ya que el generador de números aleatorios se basa en la fracción de microsegundos del tiempo actual. Además, este generador de números aleatorios no es criptográficamente seguro y el hash generado no está salado ni vinculado a una solicitud o usuario específicos.

> *«Esto se debe a que el plugin no limita correctamente la funcionalidad de*

> *simulación de roles, permitiendo que un usuario establezca su ID actual como la de un administrador si tiene acceso a un hash válido, que se puede encontrar en los registros de depuración o a través de un ataque de fuerza bruta,»* señaló Wordfence en su alerta.
>
> *«Esto permite a atacantes no autenticados suplantar su ID de usuario como la de un administrador y, posteriormente, crear una nueva cuenta de usuario con privilegios de administrador utilizando el endpoint /wp-json/wp/v2/users de la API REST.»*

Es importante destacar que esta vulnerabilidad no puede ser explotada en instalaciones de WordPress basadas en Windows, ya que la función de generación de hash depende de un método PHP llamado sys_getloadavg(), que no está implementado en Windows.

> *«Esta vulnerabilidad subraya la importancia crítica de garantizar la solidez e imprevisibilidad de los valores utilizados como hashes de seguridad o nonces,»* afirmó Muhammad.

Con una vulnerabilidad previa en LiteSpeed Cache (CVE-2023-40000, puntuación CVSS: 8.3) que ya fue explotada por actores maliciosos, es esencial que los usuarios actualicen rápidamente sus instancias a la versión más reciente.

Actualización

Wordfence ha informado que ya han comenzado los intentos de explotación de esta falla, indicando que «*bloqueó 58,952 ataques dirigidos a esta vulnerabilidad en las últimas 24 horas.*»