

Boletín de alerta

Boletín Nro.: 96

Fecha de publicación: 03/09/2026

Tema: Alerta 2026-96 Vulnerabilidad SQLi en All-in-One WP Migration and Backup

Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Producto	Versiones afectadas	Versión corregida
All-in-One WP Migration and Backup para WordPress	Todas las versiones hasta la 7.109, inclusive	7.110 o posterior

Descripción

Se identificó una vulnerabilidad de **inyección SQL de segundo orden** en el plugin de WordPress **All-in-One WP Migration and Backup** que puede derivar en la toma completa de un sitio vulnerable. El fallo, identificado como **CVE-2026-19949** y calificado con **CVSS 8.8 (Alta)**, afecta todas las versiones hasta la **7.109**, inclusive; la corrección está disponible desde la versión **7.110**.

El plugin se utiliza ampliamente para exportar, importar, restaurar y migrar sitios WordPress mediante archivos .wpress, que pueden incluir archivos de la aplicación y contenido de base de datos.

CVE-2026-19949 es una vulnerabilidad de **SQL Injection** clasificada como CWE-89 en la funcionalidad de restauración de archivos del plugin. El problema se debe a un escape insuficiente de parámetros controlados por usuarios y a la falta de preparación segura de consultas SQL existentes cuando el plugin procesa y reescribe contenido de la base de datos durante una restauración.

A diferencia de una SQLi convencional, esta falla es de **segundo orden (SQLi almacenado)**: el payload malicioso puede almacenarse inicialmente como contenido aparentemente legítimo —por ejemplo, mediante *trackbacks* aceptados por una publicación pública de WordPress— y permanecer inactivo. La carga se activa posteriormente si un administrador exporta el sitio y luego restaura/importa ese archivo con el plugin vulnerable.

Durante ese proceso, el manejo incorrecto de barras invertidas y comillas puede permitir que el contenido almacenado escape de los límites de la cadena SQL prevista y se ejecute como una consulta adicional. Esto puede permitir la extracción de información sensible de la base de datos, incluido el valor

ai1wm_secret_key, utilizado para proteger la función de importación del plugin.

Con acceso a esa clave, un atacante podría abusar de la función de importación para cargar un archivo .wordpress malicioso que contenga, por ejemplo, un plugin *must-use* (mu-plugin). Debido a que estos plugins se cargan automáticamente en WordPress, la cadena de ataque puede conducir a **ejecución remota de código (RCE)**, instalación de webshells, robo de información, despliegue de malware o toma total del sitio.



Figura 1 Condiciones para La cadena de explotación

Solución

Actualizar inmediatamente All-in-One WP Migration and Backup a la versión **7.110 o posterior**.

[All-in-One WP Migration and Backup](#)

Información adicional:

- Wordfence — *5 Million WordPress Sites Affected by SQL Injection Vulnerability in All-in-One WP Migration and Backup*
<https://www.wordfence.com/blog/2026/09/5-million-wordpress-sites-affected-by-sql-injection-vulnerability-in-all-in-one-wp-migration-and-backup-wordpress-plugin/>
- NVD — *CVE-2026-19949*
<https://nvd.nist.gov/vuln/detail/CVE-2026-19949>
- CVE Program — *CVE-2026-19949*
<https://www.cve.org/CVERecord?id=CVE-2026-19949>
- BleepingComputer — *WordPress backup plugin flaw exposes millions of sites to takeover attacks*
<https://www.bleepingcomputer.com/news/security/wordpress-backup-plugin-flaw-exposes-millions-of-sites-to-takeover-attacks/>
- Cyber Security News — *WordPress plugin flaw exposes sites to SQL injection attacks*
<https://cybersecuritynews.com/wordpress-all-in-one-wp-migration-plugin-flaw/>

- El Hacker — *Fallo en plugin All-in-One WP Migration and Backup de WordPress expone 5 millones de sitios a ataques SQLi*
<https://blog.elhacker.net/2026/09/fallo-en-plugin-all-in-one-wp-migration.html>