

Alert Bulletin

Bulletin N.: 96

Publication Date: 03/09/2026

Subject: Alert 2026-96 SQLi Vulnerability in All-in-One WP Migration and Backup

Traffic Light Protocol (TLP): White

Affected product(s):

Product	Affected versions	Fixed version
All-in-One WP Migration and Backup for WordPress	All versions up to 7.109, inclusive	7.110 or later

Description

A **second-order SQL injection** vulnerability was identified in the WordPress plugin **All-in-One WP Migration and Backup** that can lead to complete takeover of a vulnerable site. The flaw, identified as **CVE-2026-19949** and rated **CVSS 8.8 (High)**, affects all versions up to and including **7.109**; the fix is available from version **7.110**.

The plugin is widely used to export, import, restore, and migrate WordPress sites through .wpress files, which can include application files and database content.

CVE-2026-19949 is an **SQL Injection** vulnerability classified as CWE-89 in the plugin's file restoration functionality. The issue is due to insufficient escaping of user-controlled parameters and the lack of secure preparation of existing SQL queries when the plugin processes and rewrites database content during a restoration.

Unlike a conventional SQLi, this flaw is **second-order (stored SQLi)**: the malicious payload can initially be stored as seemingly legitimate content—for example, through *trackbacks* accepted by a public WordPress post—and remain dormant. The payload is subsequently activated if an administrator exports the site and then restores/imports that file with the vulnerable plugin.

During that process, improper handling of backslashes and quotes can allow the stored content to escape the bounds of the intended SQL string and execute as an additional query. This can enable extraction of sensitive information from the database, including the `ailwm_secret_key` value, used to protect the plugin's import function.

With access to that key, an attacker could abuse the import function to upload a malicious .wppress file containing, for example, a *must-use* plugin (mu-plugin). Because these plugins are loaded automatically in WordPress, the attack chain can lead to **remote code execution (RCE)**, installation of webshells, information theft, malware deployment, or full site takeover.



Figure 1 Conditions for the exploitation chain

Solution

Immediately update All-in-One WP Migration and Backup to version **7.110 or later**.

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

Additional information:

- 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 — *Flaw in WordPress plugin All-in-One WP Migration and Backup exposes 5 million sites to SQLi attacks*

