Critical security flaw in popular WordPress plugin: update now!

News · https://kyzoe.be/en/docs/critical-security-flaw-in-wordpress-plugin-update-now/

More than 900,000 WordPress websites are at risk due to a serious vulnerability in the WPvivid Backup & Migration plugin. Is your website vulnerable too?

What is going on?

Security researchers have discovered a dangerous vulnerability in the WPvivid Backup & Migration plugin for WordPress. This plugin is used by more than 900,000 websites worldwide to create backups and migrate websites to another hosting environment.

The vulnerability — officially known as **CVE-2026-1357** — has been given a severity score of **9.8 out of 10**. That is practically the maximum. An attacker without any access to your website can exploit this flaw to upload malicious files and gain full control of your website.

How exactly does the vulnerability work?

You don't need to be a technical expert to understand the essence: the plugin has two flaws at the same time.

Firstly, something goes wrong with how the plugin encrypts keys and passwords. If a certain step in that process fails, the plugin does not stop — it simply carries on with a predictable "fake key". An attacker who knows this can use it to send fake files that the plugin treats as legitimate.

Secondly, the plugin does not properly check the file names of uploaded files. As a result, an attacker can place files outside the protected folder — including malicious PHP files that can be used to take over the website from the inside.

Are you vulnerable?

Not every user of the plugin is at the same risk. You are **only critically vulnerable** if you have enabled the "*receive backup from another website*" option. This is disabled by default, but many website administrators switch it on when migrating a website from one hosting environment to

another.

In addition, an attacker has a window of only 24 hours to exploit it, because the key needed for the attack expires after one day. Even so, this is no reason to sit back: if you regularly use the plugin for migrations, you keep opening this window again and again.

What should you do?

The advice is clear: **update the WPvivid plugin to version 0.9.124 or higher immediately.**

This update was released on 28 January and contains three concrete improvements:

- The plugin now stops correctly when encryption fails, instead of carrying on with an insecure key.
- File names are now properly checked, so attackers can no longer place files outside the secure folder.
- Only permitted file types are now accepted (such as ZIP, GZ, TAR and SQL).

Timeline at a glance

Date	What happened?
12 January	Researcher Lucas Montes (NiRoX) discovers the vulnerability and reports it
22 January	Security company Defiant informs the developer WPVividPlugins
28 January	Version 0.9.124 with the fix is released

Conclusion

This is a serious vulnerability that you should not ignore. The risk of exploitation is real, especially if you use the plugin for website migrations. Check today which version of WPvivid you are using and update if necessary.

Do you need help securing your WordPress website, or would you like to know whether your website is vulnerable? **Contact Kyzoe** — we'll be happy to help.

Source: Defiant / Wordfence Security Research