Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

One Million WordPress Sites at Risk: Avada Builder Flaws Expose Sensitive Data

Date of Publication	Admiralty Code	TA Number
May 19, 2026	A1	TA2026137

Summary

First Seen: March 21, 2026
Affected Product: WordPress Plugin ThemeFusion Avada Builder (versions up to and including 3.15.2)
Impact: Two newly disclosed vulnerabilities in the widely used Avada Builder plugin have placed nearly one million WordPress websites at risk, exposing them to file theft and database compromise. The flaws, tracked as CVE-2026-4782 and CVE-2026-4798, could allow attackers to access sensitive files such as wp-config.php, steal database credentials, extract password hashes, and potentially take full control of affected sites. Security researchers warn that even low-privileged users could abuse the vulnerabilities, while one of the flaws can be exploited without authentication under specific conditions. The issues have been fully patched in Avada Builder version 3.15.3, and website administrators are being urged to update immediately to prevent data exposure and potential site compromise.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA KEV	PATCH
CVE-2026-4782	WordPress Avada Builder Arbitrary File Read via custom_svg Shortcode Parameter Vulnerability	WordPress ThemeFusion Avada Builder	✗	✗	✓
CVE-2026-4798	WordPress Avada Builder Unauthenticated SQL Injection via product_order Parameter Vulnerability	WordPress ThemeFusion Avada Builder	✗	✗	✓

Vulnerability Details

#1

Two security flaws in the Avada Builder plugin for WordPress, used on nearly one million websites, could allow attackers to access sensitive server files and extract confidential database information. Avada Builder is a widely used drag-and-drop page builder designed for the Avada theme, enabling users to create and customize website layouts without needing coding knowledge. Researchers warn that the vulnerabilities could expose critical site data and potentially lead to full website compromise if left unpatched.

#2

The first flaw, tracked as CVE-2026-4782, is an authenticated arbitrary file read issue caused by improper path validation in the plugin's fusion_get_svg_from_file() function. The vulnerability affects Avada Builder versions up to and including 3.15.2 and can be exploited by any authenticated user with Subscriber-level access or higher. Because the plugin fails to properly restrict file paths, attackers can request sensitive files stored on the server, including the highly critical wp-config.php file. Exposure of this file could reveal database credentials, authentication salts, and cryptographic keys, potentially allowing attackers to hijack sessions, create rogue administrator accounts, and maintain persistent access to compromised websites.

#3

The second issue, CVE-2026-4798, is a high-severity time-based blind SQL injection vulnerability affecting Avada Builder versions up to 3.15.1. The flaw exists in the plugin's post_query() function, where user-controlled input from the product_order parameter is inserted directly into an SQL query without proper sanitization. Although the plugin applies sanitize_text_field(), that protection is ineffective against SQL injection in this context. Under specific conditions, particularly when the WooCommerce plugin had previously been installed and later deactivated, unauthenticated attackers could exploit the flaw to slowly extract sensitive database information, including usernames and password hashes, through timing-based queries.

#4

The vulnerabilities were responsibly disclosed to Wordfence in March 2026 and later reported to the Avada Builder developers. A partial fix for the SQL injection flaw was introduced in version 3.15.2 on April 13, 2026, while the fully patched release, version 3.15.3, was issued on May 12, 2026. Website owners and administrators using Avada Builder are strongly advised to upgrade to version 3.15.3 immediately to protect their sites from potential exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-4782	WordPress ThemeFusion Avada Builder (up to and including 3.15.2)	cpe:2.3:a:theme-fusion:avada_builder:*:*:*:*:*:*:wordpress:*:*	CWE-22
CVE-2026-4798	WordPress ThemeFusion Avada Builder (up to and including 3.15.1)	cpe:2.3:a:theme-fusion:avada_builder:*:*:*:*:*:*:wordpress:*:*	CWE-89

Recommendations

Update Avada Builder to Version 3.15.3 Immediately: All WordPress sites running the Avada theme should update Avada Builder to version 3.15.3 or later without delay. This version contains the complete fix for both vulnerabilities. Because the plugin is bundled with the theme, administrators should ensure their Avada theme license is current to receive the update through the standard WordPress update mechanism.

Rotate Database Credentials and WordPress Salts: Any site that was running a vulnerable version of Avada Builder should treat wp-config.php as potentially compromised. Rotate the database password in your hosting control panel and update the DB_PASSWORD value in wp-config.php to match. Regenerate all eight WordPress authentication keys and salts using the official WordPress salt generator and replace the existing values in wp-config.php. This invalidates any forged sessions that may have been created using leaked cryptographic material.

Audit for Unauthorized Administrator Accounts and Modified Files: Review the WordPress user list for any unfamiliar administrator accounts that may have been created through exploitation. Remove any suspicious accounts immediately and reset passwords for all legitimate administrative users. Perform a file integrity check on WordPress core files and the Avada theme directory to identify any unauthorized modifications or planted backdoors.

Restrict User Registration and Enforce Least Privilege: If open user registration is enabled on the site, evaluate whether it is necessary. The arbitrary file read vulnerability requires only Subscriber-level access, making sites with open registration particularly exposed. Disable unnecessary registration or implement approval-based workflows and ensure that default roles are set to the lowest privilege level required.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
Collection	T1005: Data from Local System	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://themeforest.net/item/avada-responsive-multipurpose-theme/2833226

References

https://www.wordfence.com/blog/2026/05/1000000-wordpress-sites-affected-by-arbitrary-file-read-and-sql-injection-vulnerabilities-in-avada-builder-wordpress-plugin/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

May 19, 2026 • 9:30 PM

More at www.hivepro.com