WPBakery WordPress Vulnerability Lets Attackers Inject Malicious Code via @sejournal, @martinibuster



An advisory was issued for the popular WPBakery plugin that’s bundled in thousands of WordPress themes. The vulnerability enables authenticated attackers to inject malicious scripts that execute when someone visits an affected page.

WPBakery Plugin

WPBakery is a drag-and-drop page builder plugin for WordPress that enables users to easily create custom layouts and websites without writing code. WPBakery is frequently bundled with premium themes. Theme developers license it so that they can bring the power of a drag and drop page builder functionality to their WordPress themes.

WPBakery Vulnerability

The WPBakery Page Builder WordPress plugin was discovered to have insufficient input sanitization and output escaping in it’s Custom JS module.

Insufficient input sanitization and output escaping are flaws that enable attackers to upload malicious code into a website and cause the affected site to output malicious code. In general, this can lead to vulnerabilities such as Cross-Site Scripting (XSS) and SQL Injection.

- Input Sanitization filters uploaded user data before it is stored or processed by the plugin.
- Output Escaping converts characters that have HTML meanings into safe output before it is displayed on a web page. This prevents executable code from outputting onto a live web page and affecting users.

This flaw enables attackers with contributor-level access or higher to inject arbitrary scripts to affected websites. The vulnerability affects WPBakery plugin versions up to and including version 8.6.1.

Users of the plugin are encouraged to update to the latest version of WPBakery, which is currently version 8.7.

Featured Image by Shutterstock/3d artwork wallpaper

https://www.searchenginejournal.com/wp-bakery-wordpress-vulnerability-2/558261/