

WooCommerce Customer Review Plugin Vulnerability Affects 80,000+ Sites via @sejournal, @martinibuster

An advisory was issued about a vulnerability in the Customer Reviews for WooCommerce plugin, which is installed on over 80,000 websites. The plugin enables unauthenticated attackers to launch a stored cross-site scripting attack.

Customer Reviews for WooCommerce Vulnerability

The Customer Reviews for WooCommerce plugin enables users to send customers an email reminder to leave a review and also offers other features designed to increase customer engagement with a brand.

Wordfence issued an advisory about a flaw in the plugin that makes it possible for attackers to inject scripts into web pages that execute whenever a user visits the affected page.

The exploit is due to a failure to “sanitize” inputs and “escape” outputs. Sanitizing inputs in this context is a basic WordPress security measure that checks if uploaded data conforms to expected types and removes dangerous content like scripts. Output escaping is another security measure that ensures any special characters produced by the plugin aren’t executable.

According to the official Wordfence advisory:

“The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘author’ parameter in all versions up to, and including, 5.80.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.”

Users of the plugin are advised to update to version 5.81.0 or newer version.

Featured Image by Shutterstock/Brilliant Eye

<https://www.searchenginejournal.com/woocommerce-customer-review-plugin-vulnerability-affects-80000-sites/552544/>