

WordPress Scraper Plugin Compromised By Security Vulnerability via @sejournal, @martinibuster

A WordPress plugin that automatically posts content scraped from other websites has been discovered to contain a critical vulnerability that allows anyone to upload malicious files to affected websites. The severity of the vulnerability is rated at 9.8 on a scale of 1-10.

Crawlomatic Multisite Scraper Post Generator Plugin for WordPress

The Crawlomatic WordPress plugin is sold via the Envato CodeCanyon store for \$59 per license. It enables users to crawl forums, weather statistics, articles from RSS feeds, and directly scrape the content from other websites and then automatically publish the content on the user's website.

The plugin's Envato CodeCanyon web page features a banner that notes that the author of the plugin has been recognized for having met "WordPress quality standards" and displays a badge indicating that it is "Envato WP Requirements Compliant," an indication that it meets Envato's "security, quality, performance and coding standards in WordPress plugins and themes."

The plugin's directory page explains that it can crawl and scrape virtually any website, including JavaScript-based sites, promising that it can turn a user's website into a

“money making machine.”

Unauthenticated Arbitrary File Upload

The Crawlomatic WordPress plugin is missing a filetype validation check in all version prior to and including version 2.6.8.1.

According to a warning posted on Wordfence:

“The Crawlomatic Multipage Scraper Post Generator plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the crawlomatic_generate_featured_image() function in all versions up to, and including, 2.6.8.1. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site’s server which may make remote code execution possible.”

Users of the plugin are recommended by Wordfence to update to at least version 2.6.8.2.

Read more at Wordfence:

Crawlomatic Multipage Scraper Post Generator <= 2.6.8.1 – Unauthenticated Arbitrary File Upload

Featured Image by Shutterstock/nakaridore

<https://www.searchenginejournal.com/wordpress-scraper-plugin-compromised-by-security-vulnerability/546974/>