WordPress Contact Form Entries Plugin Vulnerability Affects 70K Websites via @sejournal, @martinibuster

A vulnerability advisory was issued for a WordPress plugin that saves contact form submissions. The flaw enables unauthenticated attackers to delete files, launch a denial of service attack, or perform remote code execution. The vulnerability was given a severity rating of 9.8 on a scale of 1 to 10, indicating the seriousness of the issue.

Database for Contact Form 7, WPForms, Elementor Forms Plugin

The Database for Contact Form 7, WPForms, Elementor Forms, also apparently known as the Contact Form Entries Plugin, saves contact form entries into the WordPress database. It enables users to view contact form submissions, search them, mark them as read or unread, export them, and perform other functions. The plugin has over 70,000 installations.

The plugin is vulnerable to PHP Object Injection by an unauthenticated attacker, which means that an attacker does not need to log in to the website to launch the attack.

A PHP object is a data structure in PHP. PHP objects can be turned into a sequence of characters (serialized) in order to store them and then deserialized (turned back into an object). The flaw that gives rise to this vulnerability is that the plugin allows an unauthenticated attacker to inject an

untrusted PHP object.

If the WordPress site also has the Contact Form 7 plugin installed, then it can trigger a POP chain during deserialization.

According to the Wordfence advisory:

> *"This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain in the Contact Form 7 plugin, which is likely to be used alongside, allows attackers to delete arbitrary files, leading to a denial of service or remote code execution when the wp-config.php file is deleted."*

All versions of the plugin up to and including 1.4.3 are vulnerable. Users are advised to update their plugin to the latest version, which as of this date is version 1.4.5.

Featured Image by Shutterstock/tavizta

https://www.searchenginejournal.com/wordpress-contact-form-entries-plugin-vulnerability-affects-70k-websites/553546/