Redirection For Contact Form 7 WordPress Plugin Vulnerability via @sejournal, @martinibuster

A vulnerability in the popular WordPress Contact Form 7 plugin addon installed in over 300,000 websites enables attackers to upload malicious files and makes it possible for them to copy files from the server.

Redirection For Contact Form 7

The Redirection for Contact Form 7 WordPress plugin by Themeisle is an add-on to the popular Contact Form 7 plugin. It enables websites to redirect site visitors to any web page after a form submission, as well as store information in a database and other functions.

Vulnerable To Unauthenticated Attackers

What makes this vulnerability especially concerning is that it is an unauthenticated vulnerability, which means that an attacker doesn't need to log in or acquire any level user privilege (like subscriber level). This makes it easier for an attacker take advantage of a flaw.

According to Wordfence:

> *"The Redirection for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type*

> *validation in the 'move_file_to_upload' function in all versions up to, and including, 3.2.7. This makes it possible for unauthenticated attackers to copy arbitrary files on the affected site's server. If 'allow_url_fopen' is set to 'On', it is possible to upload a remote file to the server."*

That last part of the vulnerability is what makes exploiting it a little harder. 'allow_url_fopen' controls how PHP handles files. PHP ships with this set to "On" but most shared hosting providers routinely set this to "Off" in order to prevent security vulnerabilities.

Although this is an unauthenticated vulnerability which make it easier to take advantage, the fact that it relies on the PHP 'allow_url_fopen' setting to be "on" mitigates the likelihood of the flaw being exploited.

Users of the plugin are encouraged to update to version 3.2.8 of the plugin or newer.

Featured Image by Shutterstock/katalinks

https://www.searchenginejournal.com/redirection-for-contact-form-7-wordpress-plugin-vulnerability/563883/