Computer Emergency Response Team of Mauritius

A Department of the Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Date of Issue: 14 August 2025

Critical WordPress Plugin Vulnerability Puts Websites at Risk of Remote Code Execution and Data Theft

Description

A critical vulnerability has been discovered in a popular WordPress plugin used by over 70,000 websites worldwide, potentially exposing them to complete takeover by malicious actors. Tracked as CVE-2025-7384, the vulnerability affects the "Database for Contact Form 7, WPforms, Elementor forms" plugin.

It is to be noted that the vulnerability requires no authentication, making it particularly accessible to threat actors. Affected websites face multiple risks, including data theft, website defacement, malware installation, and complete server compromise.

The plugin's popularity among WordPress developers, particularly those working with popular form builders like Contact Form 7, WPforms, and Elementor, significantly amplifies the potential impact.

CERT-MU advises web administrators to treat this vulnerability as a high-priority security incident requiring immediate attention, given the severity and ease of exploitation.

Affected System

The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.4.3 via deserialization of untrusted input in the get_lead_detail function.

Workaround

- CERT-MU advises website administrators using the affected plugin to immediately update to version 1.4.4 or later, which contains patches for this critical vulnerability.

More information about the patch is available on: https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/contact-form-entries/database-for-contact-form-7-wpforms-elementor-forms-143-unauthenticated-php-object-injection-to-arbitrary-file-deletion

- It is also recommended that administrators implement additional monitoring for unusual file system changes and conduct thorough security audits of any sites running the vulnerable plugin versions.

Report Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS+ - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Tel: 460 3010
Hotline No: (+230) 800 2378
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.org.mu
MAUCORS: http://maucors.govmu.org