مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in GiveWP Plugin

Tracking #:432316731

Date:13-01-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been identified in the GiveWP plugin, one of the most widely used WordPress tools for managing online donations.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-22777) has been discovered in the GiveWP WordPress plugin, affecting versions 3.19.3 and below. This flaw, with a CVSS score of 9.8, allows unauthenticated attackers to perform PHP Object Injection, potentially leading to remote code execution and full site takeover. The vulnerability impacts over 100,000 active WordPress installations using the GiveWP plugin for donation and fundraising purposes.
The vulnerability (CVE-2025-22777) in GiveWP allows unauthenticated PHP Object Injection due to insecure storage of metadata in the database. This flaw can be exploited to bypass security mechanisms and potentially take over WordPress sites.

Technical Details:

- The vulnerability stems from a weak regex check of strings, allowing attackers to bypass serialized content validation.
- Attackers can inject malicious payloads by inserting special character sequences (e.g., %25F0%259F%2598%25BC) to bypass the regex validation.
- The critical exploit scenario involves the company field in donation forms, where injected payloads can be stored as metadata and later deserialized.
- Successful exploitation can lead to arbitrary file deletion, including critical files like wp-config.php, potentially resulting in full site takeover and remote code execution.
- The vulnerability builds upon a previous flaw (CVE-2024-5932) that was patched in version 3.14.2

Fixed Version:

- GiveWP 3.19.4

RECOMMENDATIONS:

- Ensure that the GiveWP plugin is updated to fixed version or later, which patches the vulnerability.
- Review all systems running the GiveWP plugin for signs of exploitation. Check for unexpected modifications, particularly related to wp-config.php or other critical files.
- Consider deploying a Web Application Firewall (WAF) that can detect and block malicious payloads before they reach the server.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://wordpress.org/plugins/give/