مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in WPML Plugin

Tracking #:432316187

Date:27-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical Remote Code Execution Vulnerability, identified as CVE-2024-6386, has been discovered in WPML (WordPress Multilingual Plugin).

TECHNICAL DETAILS:

A critical remote code execution vulnerability, identified as CVE-2024-6386, has been discovered in the WPML (WordPress Multilingual Plugin) affecting all versions up to and including 4.6.12. This vulnerability arises from a failure to properly validate and sanitize input in the Twig template rendering process, allowing authenticated attackers to inject and execute malicious code on the server. Given WPML's widespread usage among WordPress sites for multilingual content management, the potential impact is significant. Website administrators are urged to take immediate action to mitigate risks associated with this vulnerability.

- **CVE ID:** CVE-2024-6386
- **Affected Plugin:** WPML (sitepress-multilingual-cms)
- **Affected Versions:** All versions up to 4.6.12
- **Severity:** Critical (CVSS Score: 9.9)
- **Vulnerability Type:** Remote Code Execution via Server-Side Template Injection (SSTI)
- **Fully Patched Version:** 4.6.13

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the patched version of WPML Plugin at the earliest.

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://www.wordfence.com/blog/2024/08/1000000-wordpress-sites-protected-against-unique-remote-code-execution-vulnerability-in-wpml-wordpress-plugin/