



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in WordPress Plugins

Tracking #:432316158

Date:19-08-2024

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 INTELLIGENCE 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, identified as CVE-2024-6500, has been discovered in two widely used WordPress plugins, InPost PL and InPost for WooCommerce.

TECHNICAL DETAILS:

A critical vulnerability, identified as **CVE-2024-6500**, has been discovered in two widely used WordPress plugins, InPost PL and InPost for WooCommerce, affecting over 10,000 sites. This flaw, which has a **CVSS score of 10**, allows for arbitrary file reading and deletion, posing a significant risk of complete site takeover. The InPost for WooCommerce plugin is removed from the WordPress.org repository.

- **CVE ID:** CVE-2024-6500
- **CVSS Score:** **10.0 (Critical)**
- **Description:** InPost for WooCommerce <= 1.4.0 and InPost PL <= 1.4.4 - Missing Authorization to Unauthenticated Arbitrary File Read and Delete
- **Affected Plugins:** InPost PL, InPost for WooCommerce
- **Affected Versions:** <= 1.4.4 (for InPost PL), <= 1.4.0 (for InPost for WooCommerce)
- **Fully Patched Version:** 1.4.5 (for InPost PL).

RECOMMENDATIONS:

- **Immediate Plugin Update:** Users of the InPost PL plugin should upgrade to version 1.4.5 without delay.
- **Uninstall InPost for WooCommerce:** Since this plugin has been removed from the repository, users must uninstall it and transition to InPost PL.
- **Conduct Security Audits:** Perform a thorough review of all plugins and themes in use to identify any additional vulnerabilities.
- **Implement Regular Backups:** Ensure that regular backups are conducted to recover from potential data loss due to exploitation.
- **Enhance Monitoring:** Deploy monitoring solutions to detect unusual activities or unauthorized access attempts on WordPress sites.

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/threat-intel/vulnerabilities/detail/inpost-for-woocommerce-140-and-inpost-pl-144-missing-authorization-to-unauthenticated-arbitrary-file-read-and-delete>