مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in WordPress File Upload Plugin

Tracking #:432316716

Date:08-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been discovered in the WordPress File Upload plugin that allows unauthenticated attackers to execute remote code, read arbitrary files, and delete files on affected WordPress sites.

TECHNICAL DETAILS:

A critical vulnerability (CVE-2024-11613) has been discovered in the WordPress File Upload plugin, affecting all versions up to and including 4.24.15. This vulnerability allows unauthenticated attackers to execute remote code, read arbitrary files, and delete files on affected WordPress sites.

- CVE ID: **CVE-2024-11613**
- CVSS Score: 9.8 (Critical)
- Vulnerability: Unauthenticated Remote Code Execution, Arbitrary File Read, and Arbitrary File Deletion
- Affected Versions: WordPress File Upload plugin <= 4.24.15
- Patched Version: 4.25.0

RECOMMENDATIONS:

- Upgrade the WordPress File Upload plugin to the fixed version at the earliest.
- Review server logs for any suspicious file access or modifications.

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/wordpress-plugins/wp-file-upload/wordpress-file-upload-42415-unauthenticated-remote-code-execution-arbitrary-file-read-and-arbitrary-file-deletion