



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Vulnerability in WP Umbrella WordPress Plugin

Tracking #:432316608

Date:09-12-2024

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 security vulnerability in the popular WordPress plugin, WP Umbrella. This flaw could potentially allow unauthenticated attackers to take complete control of affected websites.

TECHNICAL DETAILS:

A critical security vulnerability (CVE-2024-12209) with a CVSS score of 9.8 has been discovered in the WP Umbrella: Update Backup Restore & Monitoring plugin for WordPress, affecting all versions up to and including 2.17.0. This vulnerability exposes over 30,000 websites to potential compromise.

Vulnerability Details:

- **CVE-2024-12209**
- CVSS score of 9.8 **Critical**
- A critical vulnerability exists in the WP Umbrella plugin for WordPress. This Local File Inclusion vulnerability allows unauthenticated attackers to include and execute arbitrary files on the server via the 'filename' parameter of the 'umbrella-restore' action.
- The vulnerability enables attackers to bypass access controls, obtain sensitive data, and potentially achieve code execution. This poses significant risks to affected websites, including:
 - Unauthorized access to admin accounts
 - Data breaches
 - Malware installation
 - Potential for broader cyberattacks

Affected Versions:

- All versions up to and including 2.17.0.

Fixed Versions:

- Update to version 2.17.1, or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions 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://nvd.nist.gov/vuln/detail/CVE-2024-12209>