مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in InstaWP Connect WordPress Plugin

Tracking #:432317100
Date:18-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the InstaWP Connect WordPress plugin, which is used for staging and migrating WordPress sites. This vulnerability could allow attackers to execute arbitrary files on the server, potentially compromising entire websites.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-2636**
- CVSS score 9.8 Critical
- A critical vulnerability exists in the InstaWP Connect WordPress plugin. This flaw is an unauthenticated Local PHP File Inclusion (LFI) vulnerability within the instawp-database-manager parameter. This vulnerability allows unauthenticated attackers to include and execute arbitrary files on the server hosting the affected WordPress website.
- Malicious actors can use this vulnerability to:
  - Bypass access controls, gaining unauthorized administrative privileges.
  - Steal sensitive data, such as user credentials and confidential information.
  - Execute arbitrary code, enabling full takeover of affected websites.
  - Upload and execute files, using innocent-looking files (e.g., images) to achieve remote access.

Affected Versions

- All versions of InstaWP Connect up to 0.1.0.85

Fixed Versions:

- InstaWP Connect v0.1.0.86 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by InstaWP Connect.

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-2025-2636