مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in UpdraftPlus WP Backup & Migration Plugin

Tracking #:432316711

Date:07-01-2025

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 INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the UpdraftPlus WP Backup & Migration Plugin that could be exploited by attackers to gain full control of affected websites.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-10957**
- CVSS score 8.8 High
- A security vulnerability exists in the UpdraftPlus WP Backup & Migration Plugin, which could allow unauthenticated attackers to exploit PHP Object Injection vulnerabilities under specific conditions.
- The vulnerability exists in the 'recursive_unserialized_replace' function, which improperly handles deserialization of untrusted input. While no known PHP Object POP (Property-Oriented Programming) chain exists in the plugin itself, if additional vulnerable plugins or themes are present, attackers could potentially:
    - Delete arbitrary files
    - Access sensitive data
    - Execute arbitrary code

Exploit Conditions:

Exploitation of this vulnerability requires:

- An administrator to perform a search-and-replace operation within the UpdraftPlus plugin.
- The presence of vulnerable third-party plugins or themes that enable exploitation through a POP chain.

Successful exploitation of this vulnerability could lead to:

- **File Deletion**: Attackers could delete critical website files, disrupting functionality or rendering the site offline.
- **Data Theft**: Sensitive information, such as user credentials, database configurations, or financial records, could be accessed and stolen.
- **Code Execution**: Attackers could execute arbitrary code, gaining full control of the website to distribute malware, deface the site, or launch further attacks.

Affected Versions:

- UpdraftPlus up to and including **1.24.11**.

Fixed Versions:

- UpdraftPlus **1.24.12** 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-2024-10957