مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Alone WordPress Theme

Tracking #:432317557
Date:31-07-2025

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

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution vulnerability in the 'Alone – Charity Multipurpose Non-profit' WordPress theme that is being actively exploited in the wild. Unauthenticated attackers are leveraging this flaw to upload arbitrary files and compromise thousands of WordPress sites

TECHNICAL DETAILS:

The vulnerability stems from the improper implementation of the alone_import_pack_install_plugin() function, which lacks both capability and nonce checks. This AJAX action is exposed to unauthenticated users via the nopriv hook, allowing attackers to install plugins from remote sources. Exploitation enables attackers to upload malicious PHP files, leading to full site compromise.

Vulnerability Details:

- **Vulnerability ID**: CVE-2025-5394
- **CVSS Score**: 9.8
- **Severity**: Critical
- **Type**: Remote Code Execution (RCE) via Arbitrary File Upload
- **Affected Component**: alone_import_pack_install_plugin() function
- **Affected Versions**: Versions prior to 7.8.5
- **Fixed Version**: 7.8.5 and later

Indicators of Compromise: Refer to Wordfence

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Vendor.

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/blog/2025/07/attackers-actively-exploiting-critical-vulnerability-in-alone-theme/