مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in OttoKit WordPress Plugin

Tracking #:432317220

Date:06-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the OttoKit WordPress plugin that could be exploited to gain full administrative access to affected WordPress sites, potentially resulting in complete site compromise.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-27007**
- CVSS Score: 9.8 Critical
- A Privilege Escalation vulnerability in the OttoKit WordPress plugin this flaw allows attackers to gain administrator privileges without authentication.
- The vulnerability is caused by insufficient authentication validation in OttoKit's REST API, making it possible for attackers to elevate privileges without proper authorization.
- Exploitation of this vulnerability can lead to:
  - **Complete takeover of affected websites**, allowing attackers to modify content, steal data, and disrupt services.
  - **Unauthorized creation of administrator accounts**, enabling persistent control by malicious actors.
  - **Potential data breaches**, compromising customer and business information stored on the site.
  - **Increased risk of further exploitation**, including malware installation or spreading phishing attacks.

Affected Versions:

- OttoKit WordPress Plugin (versions before 1.0.83)

Fixed Versions:

- OttoKit version 1.0.83 or later

RECOMMENDATIONS:

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

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-2025-27007