مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Privilege Escalation Vulnerability in Post SMTP WordPress Plugin

Tracking #:432317535

Date:25-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Post SMTP WordPress Plugin. This flaw enables attackers to hijack administrator accounts and gain full control of the affected WordPress site.

TECHNICAL DETAILS:

The vulnerability arises from broken access control in the plugin's REST API, specifically in the *get_logs_permission* function. This function only checks if a user is logged in, without validating their privilege level. As a result, even Subscriber-level users can access sensitive API endpoints, including:

- Viewing full email logs (including message bodies)
- Resending emails
- Viewing email statistics
- Intercepting password reset emails

Vulnerability Details:

- **Vulnerability ID:** CVE-2025-24000
- **Severity:** High
- **CVSS Score:** 8.8
- **Impact:** Full Site Takeover via Privilege Escalation
- **Affected Component:** Post SMTP WordPress Plugin
- **Vulnerable Versions:** 3.2.0 and below
- **Fixed Version:** 3.3.0

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released 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://patchstack.com/articles/account-takeover-vulnerability-affecting-over-400k-installations-patched-in-post-smtp-plugin/