

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High-Severity Vulnerability in RealHomes WordPress Theme

Tracking #:432317359

Date:10-06-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the RealHomes WordPress theme. This vulnerability could allow low-privilege authenticated users to escalate their roles to administrator, leading to potential complete site compromise.

TECHNICAL DETAILS:

A critical privilege escalation vulnerability has been identified in the RealHomes WordPress theme, affecting versions prior to 4.4.1. This vulnerability allows authenticated users with subscriber-level access or higher to escalate their privileges to administrator, potentially leading to complete site compromise.

Vulnerability Details:

- **CVE-2025-4601**
- **CVSS Score:** 8.8 (High)
- **Vulnerability Type:** Privilege Escalation
- The `inspiry_update_profile()` function allows users to change their own user role via the profile form, if the "Show user role option in profile" setting is enabled. There are no restrictions on which roles can be selected.

Impact

- **Unauthorized Privilege Escalation:** Low-privilege users can grant themselves administrator rights.
- **Site Compromise:** Attackers can upload malicious files, inject backdoors, modify or delete content, redirect visitors, and insert spam or phishing pages.
- **Exploitability:** The vulnerability is exploitable with minimal initial access (subscriber account).

Affected Versions:

- RealHomes WordPress Theme (RH - Real Estate WordPress Theme): All versions up to, and including, 4.4.0

Fixed Version:

- RealHomes Theme (RH - Real Estate WordPress Theme) version 4.4.1 or later.

RECOMMENDATIONS:

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

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/2025/06/33000-wordpress-sites-affected-by-privilege-escalation-vulnerability-in-realhomes-wordpress-theme/>