مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

# Actively Exploited Vulnerability in Case Theme User Plugin

Tracking #:432317714

Date:15-09-2025

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the Case Theme User plugin that is being actively exploited to gain unauthorized access to affected websites.

## TECHNICAL DETAILS:

A critical authentication bypass vulnerability has been identified in the Case Theme User WordPress plugin, which is bundled in several premium WordPress themes. This flaw, tracked as CVE-2025-5821, allows unauthenticated attackers to gain administrative access to vulnerable websites. Exploitation has been observed in the wild.

**Vulnerability Details**

- **CVE-2025-5821**
- **CVSS Score:** 9.8 (Critical)
- **Vulnerability:** Authentication Bypass
- **Root Cause:** The plugin's facebook_ajax_login_callback() function mishandles authentication logic for Facebook-based social login.
- **Impact:** Successful exploitation may allow attackers to log in as any user, including administrator accounts, if the target email address is known or guessable.
- **Affected Versions:** Case Theme User ≤ 1.0.3
- **Fixed Version:** Case Theme User 1.0.4 or later

**Exploitation Activity**

- Attackers create temporary user accounts, exploit the bypass to escalate privileges to administrator, then remove the temporary accounts to erase traces.
- Commonly targeted
  emails: owner@domain.com, office@domain.com, sales@domain.com.

**Indicators of Compromise (IOCs):**

- 2602[:]ffc8[:]2[:]105[:]216[:]3cff[:]fe96[:]129f
- 146[.]70[.]186[.]142
- 107[.]175[.]179[.]8
- 2602[:]ffc8[:]2[:]105[:]216[:]3cff[:]fe40[:]4b78
- 89[.]117[.]42[.]68

## RECOMMENDATIONS:

- Update Immediately: Upgrade to Case Theme User version 1.0.4 or later.
- Audit Accounts: Review all administrator and privileged accounts for unauthorized creation or logins.
- Log Review: Check webserver and WordPress logs for suspicious AJAX activity and attempts from known malicious IPs.
- Credential Security: Reset administrator passwords and enforce strong authentication.
- WAF Deployment: Apply Web Application Firewall (WAF) rules to block known malicious activity.
- Incident Response: If compromise is suspected, perform a full forensic review and restore from a verified clean backup.

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/2025/09/attackers-actively-exploiting-critical-vulnerability-in-case-theme-user-plugin/
- https://nvd.nist.gov/vuln/detail/CVE-2025-5821