

مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**RCE Vulnerability in Craft CMS**

Tracking #:432317643

Date:27-08-2025

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 INTELLIGENCE 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 moderate-severity vulnerability has been identified in Craft CMS allowing potential remote code execution (RCE) through Server-Side Template Injection (SSTI) in Twig templates.

## TECHNICAL DETAILS:

A moderate-severity vulnerability has been identified in Craft CMS (versions 4.x and 5.x), allowing potential remote code execution (RCE) through Server-Side Template Injection (SSTI) in Twig templates.

### Vulnerability Details

- **CVE ID:** CVE-2025-57811
- **GHSA ID:** GHSA-crcq-738g-pqvc
- **Severity:** Moderate
- **Attack Vector:** Network
- **Attack Complexity:** Low
- **Privileges Required:** High
- **User Interaction:** None
- **Impact:**
  - **Confidentiality:** High
  - **Integrity:** High
  - **Availability:** High

### CVSS v4.0 Vector:

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P

### Weaknesses:

- **CWE-22:** Path Traversal
- **CWE-94:** Code Injection
- **CWE-1336:** Improper Neutralization of Special Elements in Templates

### Exploit Prerequisites:

- Admin access
- **ALLOW\_ADMIN\_CHANGES** enabled

### Patched Versions:

- 4.16.6
- 5.8.7

## RECOMMENDATIONS:

- Update Craft CMS to patched versions immediately and enforce secure configuration to prevent exploitation.

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://github.com/advisories/GHSA-crcq-738g-pqvc>