مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Remote Code Execution (RCE) Vulnerability in Craft CMS
Tracking #:432318213
Date:06-01-2026

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity authenticated Remote Code Execution (RCE) vulnerability has been identified in Craft CMS.

TECHNICAL DETAILS:

A high-severity authenticated Remote Code Execution (RCE) vulnerability has been identified in Craft CMS, affecting both 4.x and 5.x branches. The flaw allows an authenticated administrator to achieve arbitrary command execution on the underlying server by abusing Yii's behavior attachment mechanism combined with wildcard event listeners.

The vulnerability bypasses previous mitigations for related flaws (including CVE-2024-4990) by leveraging a legitimate Yii Behavior class (AttributeTypecastBehavior) rather than a custom or non-Behavior class. This results in code execution through PHP Reflection and magic methods when events are triggered on crafted components.

Vulnerability Details:
- CVE ID: CVE-2025-68455
- Vulnerability Type: Authenticated Remote Code Execution (RCE)
- CVSS v3.1 Base Score:8.8 (High)
- Attack Vector: Network
- Attack Complexity: Low
- Privileges Required: High (Administrator access to Craft CMS Control Panel)
- User Interaction Required: None

Affected Product
- Package Name:
  craftcms/cms (Composer)

Affected Versions
- Craft CMS 5.x:
  - \>= 5.0.0-RC1
  - <= 5.8.20
- Craft CMS 4.x:
  - \>= 4.0.0-RC1
  - <= 4.16.16

Patched Versions
- Craft CMS 5.x:5.8.21
- Craft CMS 4.x: 4.16.17

RECOMMENDATIONS:

- Upgrade Craft CMS immediately to fixed version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/advisories/GHSA-255j-qw47-wjh5