NCSC Advisory

Critical Vulnerability in Craft CMS
CVE-2025-32432

23rd, June 2025

STATUS: TLP:CLEAR

Description

CVE ID: CVE-2025-32432

Published: 2025-04-25

Vendor: Craft CMS

Product: Craft CMS

CVSS Score[1]: 10.0

Products Affected

Product	Version
CMS	>= 3.0.0-RC1, < 3.9.15
CMS	>= 4.0.0-RC1, < 4.14.15
CMS	>= 5.0.0-RC1, < 5.6.17

Impact

Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. Starting from version 3.0.0-RC1 to before 3.9.15, 4.0.0-RC1 to before 4.14.15, and 5.0.0-RC1 to before 5.6.17, Craft is vulnerable to remote code execution. This is a high-impact, low-complexity attack vector. This issue has been patched in versions 3.9.15, 4.14.15, and 5.6.17, and is an additional fix for CVE-2023-41892.

Common Weakness Enumeration (CWE)[2]: CWE-94: Improper Control of Generation of Code ('Code Injection')

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

---

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Craft CMS.

- https://nvd.nist.gov/vuln/detail/CVE-2025-32432

- https://www.cve.org/CVERecord?id=CVE-2025-32432

- https://craftcms.com/knowledge-base/craft-cms-cve-2025-32432

- https://sensepost.com/blog/2025/investigating-an-in-the-wild-campaign-using-rce-in-craftcms/

Tom Johnson House, Beggar's Bush, Dublin 4, Ireland, D04 K7X4
T +353 (0)1 678 2333   **E** info@ncsc.gov.ie

ncsc.gov.ie

TLP: CLEAR

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre