

# CVE-2025-23209

## Craft CMS Code Injection Vulnerability

CISA KEV since Feb 20, 2025

Actively exploited

Craft is a flexible, user-friendly CMS for creating custom digital experiences on the web and beyond. This is an remote code execution (RCE) vulnerability that affects Craft 4 and 5 installs where your security key has already been compromised. Anyone running an unpatched version of Craft with a compromised security key is affected. This vulnerability has been patched in Craft 5.5.8 and 4.13.8. Users who cannot update to a patched version, should rotate their security keys and ensure their privacy to help mitigate the issue.

|                                                                           |                                                      |                                                                  |                                                                                            |
|---------------------------------------------------------------------------|------------------------------------------------------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <p>EVRS</p> <p><b>75</b><sub>/100</sub></p> <p><b>Urgent</b> priority</p> | <p>CVSS V3.1</p> <p><b>8.1</b></p> <p>High · NVD</p> | <p>EPSS</p> <p><b>0.218</b></p> <p>97.6th percentile · FIRST</p> | <p>CISA DEADLINE</p> <p><b>Mar 13, 2025</b></p> <p>KEV since 2025 · listed over a year</p> |
|---------------------------------------------------------------------------|------------------------------------------------------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                     |                                          |                                                                |                                             |
|-----------------------------------------------------|------------------------------------------|----------------------------------------------------------------|---------------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b> | Listed in the catalog                    | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild          |
| <input type="checkbox"/> <b>Ransomware</b>          | No known ransomware campaign association | <input type="checkbox"/> <b>KEV recency</b>                    | Added to CISA KEV within the last two years |
| <input checked="" type="checkbox"/> <b>EPSS</b>     | 0.218 probability                        | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable               |
| <input checked="" type="checkbox"/> <b>CVSS</b>     | Base score 8.1                           | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                         |

### Remediation

**Patch This Cycle** Patch or fixed version identified

**CISA required action:** Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

### Affected and fixed versions

| PACKAGE      | AFFECTED                                              | FIXED IN       | SOURCE |
|--------------|-------------------------------------------------------|----------------|--------|
| craftcms/cms | ≥ 5.0.0-RC1, < 5.5.5                                  | 5.5.8          | GitHub |
| craftcms/cms | ≥ 4.0.0-RC1, < 4.13.8                                 | 4.13.8         | GitHub |
| craft cms    | > 4.0.0 < 4.13.8<br>> 5.0.0 < 5.5.8<br>4.0.0<br>5.0.0 | 4.13.8 · 5.5.8 | NVD    |

### Sources

|                        |                                                                                                                                                                       |                            |                                                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor guidance</b> | <a href="https://github.com/craftcms/cms/commit/e59e22b30c9dd39e5e2c7fe02c147bcbd004e603">github.com/craftcms/cms/commit/e59e22b30c9dd39e5e2c7fe02c147bcbd004e603</a> | <b>Additional guidance</b> | <a href="https://github.com/craftcms/cms/security/advisories/GHSA-x684-96hh-833x">github.com/craftcms/cms/security/advisories/GHSA-x684-96hh-833x</a> |
| <b>NVD</b>             | <a href="https://nvd.nist.gov/vuln/detail/CVE-2025-23209">nvd.nist.gov/vuln/detail/CVE-2025-23209</a>                                                                 | <b>CISA KEV</b>            | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                               |
| <b>GitHub advisory</b> | <a href="https://github.com/advisories/GHSA-x684-96hh-833x">github.com/advisories/GHSA-x684-96hh-833x</a>                                                             | <b>ENISA EUVD</b>          | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2025-0208">euvd.enisa.europa.eu/vulnerability/EUVD-2025-0208</a>                             |
| <b>Current data</b>    | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2025-23209">evulnable.com/vulnerability-management/cve/CVE-2025-23209</a>                             |                            |                                                                                                                                                       |

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.