

CVE-2025-32432

Craft CMS Code Injection Vulnerability

Exigent

CISA KEV since Mar 20, 2026

Actively exploited

Public exploit module (Metasploit)

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.

EVRS 90/100 Immediate priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.998 99.96th percentile · FIRST	CISA DEADLINE Apr 3, 2026 CISA federal deadline · Overdue by 7 months
--	---	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.998 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, 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	≥ 3.0.0-RC1, ≤ 3.9.14	3.9.15	GitHub
craftcms/cms	≥ 4.0.0-RC1, ≤ 4.14.14	4.14.15	GitHub
craftcms/cms	≥ 5.0.0-RC1, ≤ 5.6.16	5.6.17	GitHub
craft cms	≥ 3.0.0 < 3.9.15 ≥ 4.0.0 < 4.14.15 ≥ 5.0.0 < 5.6.17	3.9.15 · 4.14.15 · 5.6.17	NVD

Sources

Vendor guidance	github.com/craftcms/cms/commit/e1c85441fa47eeb7c688c2053f25419bc0547b47	Additional guidance	github.com/craftcms/cms/security/advisories/GHSA-f3gw-9ww9-jmc3
craftcms.com	craftcms.com/knowledge-base/craft-cms-cve-2025-32432	NVD	nvd.nist.gov/vuln/detail/CVE-2025-32432
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-f3gw-9ww9-jmc3
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2025-12521	Current data	evulnable.com/vulnerability-management/cve/CVE-2025-32432

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