CVE-2025-32432: CRAFT CMS ALLOWS REMOTE CODE EXECUTION

Vairav CVE Report

Date: April 28, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A critical remote code execution (RCE) vulnerability (CVE-2025-32432) has been identified in Craft CMS, impacting versions 3.x, 4.x, and 5.x. Exploitation could allow unauthenticated attackers to execute arbitrary code, leading to full system compromise. Immediate patching is highly recommended to secure affected installations.

VULNERABILITY DETAILS

CVE-2025-32432: Craft CMS Allows Remote Code Execution

Description: Craft CMS versions from 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 are vulnerable to a remote code execution flaw. The vulnerability stems from improper control over the generation of executable code (CWE-94), allowing attackers to inject and execute malicious code remotely without authentication.

Impact: System compromise, malware deployment, or service disruption.

CVSS Score: 10.0 (Critical)

AFFECTED PRODUCTS/VERSIONS

- Craft CMS versions **3.0.0-RC1** up to (but not including) **3.9.15**
- Craft CMS versions **4.0.0-RC1** up to (but not including) **4.14.15**
- Craft CMS versions **5.0.0-RC1** up to (but not including) **5.6.17**

EXPLOIT DETAILS

Attackers can remotely send specially crafted payloads to vulnerable Craft CMS instances, exploiting the code generation flaw. No authentication or user interaction is required, making exploitation trivial and extremely dangerous for public-facing sites.

RECOMMENDATIONS

- **Immediate Upgrade:** Update Craft CMS to versions 3.9.15, 4.14.15, or 5.6.17 or later.
- **Restrict Access:** If immediate upgrading is not possible, restrict external access to Craft CMS admin panels via firewalls or VPN.
- **Monitor Systems:** Check for unusual system behavior or new files that may indicate compromise.

- **Security Best Practices:** Regularly audit servers and application configurations, apply patches timely manner, and minimize plugin use from unverified sources.

REFERENCES

https://www.cve.org/CVERecord?id=CVE-2025-32432
https://github.com/craftcms/cms/security/advisories/GHSA-f3gw-9ww9-jmc3
https://craftcms.com/knowledge-base/craft-cms-cve-2025-32432
https://securityonline.info/craft-cms-zero-day-cve-2025-32432-exploited-with-metasploit-module-now-public/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com