مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Critical Vulnerabilities in Craft CMS

Tracking #:432317341

Date:04-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed two actively exploited vulnerabilities have been disclosed in Craft CMS, a popular content management system used across industries for custom digital experiences.

TECHNICAL DETAILS:

Two actively exploited vulnerabilities have been disclosed in Craft CMS, a popular content management system used across industries for custom digital experiences.

Vulnerability Details:

1. **CVE-2024-56145 – Remote Code Execution via PHP Argv Injection**
   - CVSS Score: 9.3 (CRITICAL)
   - Attack Vector: Remote, unauthenticated
   - Exploitation Status: Confirmed in the wild
   - Vulnerable Config: register_argc_argv = On
   - Impact:
     - Attacker can execute arbitrary PHP code remotely
     - Full system compromise possible
   - Affected Versions:
     - 3.x: ≥ 3.0.0 to < 3.9.14
     - 4.x: ≥ 4.0.0-RC1 to < 4.13.2
     - 5.x: ≥ 5.0.0-RC1 to < 5.5.2
   - Fixed versions: v3.9.14, v4.13.2, or v5.5.2

2. **CVE-2025-35939 – Unsanitized Session File Injection**
   - CVSS Score: 6.9 (MEDIUM)
   - Attack Vector: Remote, unauthenticated
   - Exploitation Status: Confirmed in the wild
   - Description:
     - Craft CMS stores unauthenticated user-controlled values in session files (e.g., /var/lib/php/sessions/sess_[value])
     - Attacker may inject arbitrary PHP code into a known file path
     - Can be chained with other vulnerabilities (e.g., LFI, file include) for code execution
   - Affected Versions:
     - 4.x: < 4.15.3
     - 5.x: < 5.7.5
   - Fixed versions: v4.15.3 or v5.7.5

Status: Exploited in the Wild
Threat intelligence sources and vendor advisories confirm that both vulnerabilities have been used in targeted attacks. Systems running unpatched versions of Craft CMS may already be compromised. Immediate action is required.

RECOMMENDATIONS:

- Upgrade Craft CMS Immediately to fixed version or later as soon as possible.
- Scan for indicators of compromise:
  - Unexpected sess_* files containing executable code
  - Web shell artifacts
  - Outbound network traffic to suspicious domains/IPs
  - Review authentication logs and web access logs for anomalies

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

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

REFERENCES:

- https://www.cve.org/CVERecord?id=CVE-2024-56145
- https://www.cve.org/CVERecord?id=CVE-2025-35939