مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Zero-Day Exploit Chain Targeting Craft CMS

Tracking #:432317140

Date:28-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution (RCE) vulnerability in Craft CMS is being actively exploited in combination with an input validation flaw in the Yii framework to compromise servers, upload backdoors, and exfiltrate data.

TECHNICAL DETAILS:

A critical remote code execution (RCE) vulnerability in Craft CMS (CVE-2025-32432, CVSS 10.0) is being actively exploited in combination with an input validation flaw in the Yii framework (CVE-2024-58136) to compromise servers, upload backdoors, and exfiltrate data. Attackers chain these vulnerabilities to bypass security controls, with a public Metasploit module now lowering the barrier for exploitation. Patched versions (Craft CMS 3.9.15/4.14.15/5.6.17 and Yii 2.0.52) were released in April 2025, but unpatched systems remain at high risk.

Vulnerability Details:

- **CVE-2025-32432 10.0 CRITICAL (Craft CMS RCE):** A remote code execution vulnerability exists in Craft CMS, where an attacker can send a specially crafted HTTP request containing a "return URL" parameter. This parameter is improperly saved into a PHP session file, which is then returned in the HTTP response. Attackers can exploit this flaw to inject malicious code into the server.
- **CVE-2024-58136 9.0 CRITICAL (Yii Framework Input Validation Flaw):** An input validation vulnerability in the Yii framework, used by Craft CMS, allows attackers to send a malicious JSON payload that triggers PHP code execution on the server.

Exploit Process:

1. **Craft CMS Vulnerability:** Attackers exploit the RCE flaw in Craft CMS by sending a specially crafted HTTP request to the server.
2. **Yii Framework Vulnerability:** Once the malicious session file is created, the input validation flaw in the Yii framework is exploited to execute PHP code.
3. **Payload Execution:** The attacker installs a PHP-based file manager to gain complete control over the compromised system, allowing for data theft and further exploitation.

Impact:

- **Full Server Compromise:** Successful exploitation leads to complete system control by the attacker, allowing them to steal sensitive data, modify files, and execute arbitrary code.
- **Data Theft and Integrity Loss:** Attackers can access and exfiltrate sensitive information stored on the server, including databases, user data, and configuration files.
- **Increased Attack Surface:** The public availability of a Metasploit module further lowers the barrier for attack, making it easier for less sophisticated attackers to target vulnerable systems.

Patched Versions:

- Craft CMS: Update to versions 3.9.15, 4.14.15, or 5.6.17 to address CVE-2025-32432.
- Yii Framework: Update to version 2.0.52 to address CVE-2024-58136.

Indicators of Compromise:

IOC	Type	Description
103.106.66[.]123	IP address	Attempted to drop filemanager.php
172.86.113[.]137	IP address	Dropped filemanager.php
104.161.32[.]11	IP address	Dropped filemanager.php
154.211.22[.]213	IP address	Uploaded file using filemanager.php
38.145.208[.]231	IP address	Renamed filemanager.php
d8fddbd85e6af76c91bfa17118dbecc6	md5	File dropped at the root of the web directory
e6c3e12f6712719f69f40fb6f06e2b60facd8e61	sha1	File dropped at the root of the web directory
dce988346f98d55b97f7ca7a4c49cef2883b80855a0ecb6371df4063e7ecc40d	sha256	File dropped at the root of the web directory
autoload_classmap.php	Filename	File dropped at the root of the web directory
wp-22.php	Filename	File dropped at the root of the web directory
style.php	Filename	File dropped at the root of the web directory
https://github.com/alexantr/filemanager	github-repository	Open-source project source of filemanager.php

RECOMMENDATIONS:

- Update Craft CMS & Yii Framework to the patched version.
- Credential Rotation: Rotate all private keys, database credentials, and API keys used in the affected system to prevent unauthorized access.
- Continuously monitor logs for suspicious activity and cross-check against known IOCs, including malicious file names, IP addresses, and user agents.
- Implement security best practices such as input validation, output encoding, and strict session management to reduce exposure to similar vulnerabilities in the future.
- Ensure the use of Web Application Firewalls (WAF) and other security layers to block malicious requests that may exploit these types of vulnerabilities.

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.yiiframework.com/news/709/please-upgrade-to-yii-2-0-52
56179e4a4121d96c5dc2e4419d469b24
- https://github.com/craftcms/cms/security/advisories/GHSA-f3gw-9ww9-jmc3