مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in Krayin CRM

Tracking #:432318799

Date:16-04-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Krayin CRM, an open-source CRM platform built on Laravel and Vue.js. The flaw allows authenticated attackers to execute arbitrary code on the server, potentially leading to full system compromise.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE ID:** CVE-2026-38526
- **Severity** Critical **CVSS:** 9.9
- The vulnerability exists in the TinyMCE media upload endpoint (/admin/tinymce/upload), where uploaded files are not properly validated. The application fails to enforce MIME type and file extension restrictions and stores files directly in a web-accessible directory.
- Due to these weaknesses, an authenticated attacker can upload a malicious PHP file and execute it via a web request, resulting in Remote Code Execution (RCE) within the server environment.

Affected Products

- Krayin CRM 2.2.x

Mitigations / Workarounds

- Enforce strict allowlisting of file types (e.g., jpg, png, gif, webp)
- Validate both MIME types and file extensions
- Store uploads outside the web root (e.g., /storage/)
- Rename uploaded files using random UUIDs
- Disable script execution in upload directories (e.g., via .htaccess or Nginx configuration)
- Restrict access to the upload endpoint to privileged users only

RECOMMENDATIONS:

- Immediately apply the recommended mitigations
- Monitor logs for suspicious upload or execution activity
- Review user roles and enforce least-privilege access
- Deploy a Web Application Firewall (WAF) to detect malicious uploads
- Apply vendor patches as soon as they become available

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://nvd.nist.gov/vuln/detail/CVE-2026-38526