مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Directus

Tracking #:432317635

Date:25-08-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Directus, an open-source real-time API and dashboard for managing SQL database content. The flaw allows unauthenticated attackers to upload or modify files on vulnerable servers.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-55746**
- **CVSS Score**: 9.3 (Critical)
- The vulnerability resides in the /files route, which exposes CRUD operations for file handling. Due to insufficient sanitization of the filename_disk value, attackers can bypass safeguards and manipulate files on the server.
- **Potential Impact:**
  - Phishing Pages using crafted SVG files
  - Unauthenticated Remote Code Execution via webshell uploads
  - File Poisoning and Credential Theft through tampered internal documents
- **Affected Versions:**
  - All versions prior to 11.9.3
- **Fixed Versions:**
  - 11.9.3 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Vendor.

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://github.com/directus/directus/security/advisories/GHSA-mv33-9f6j-pfmc