مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in LibreOffice

Tracking #:432316919

Date:28-02-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in LibreOffice that could allow attackers to execute malicious files on users' systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-0514**
- CVSS score 7.2 High
- A security vulnerability in LibreOffice, affecting versions prior to 24.8.5. This vulnerability could allow attackers to execute malicious files on Windows systems by exploiting the way LibreOffice handles hyperlinks in documents
- The vulnerability stems from an improper input validation issue in LibreOffice's hyperlink handling mechanism on Windows. When a user activates a hyperlink by pressing CTRL and clicking, LibreOffice passes the link to the Windows ShellExecute function for processing. While LibreOffice has a security mechanism to block executable file paths, attackers found a way to bypass this protection using non-file URLs that mimic Windows file paths.
- Successful exploitation of this vulnerability could allow an attacker to execute arbitrary files on a user's system, potentially leading to malware infections, data breaches, or further system compromise.

Fixed Versions:

- LibreOffice 24.8.5 or later for Windows

RECOMMENDATIONS:

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

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-2025-0514