مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Vulnerabilities in LangChain Gen AI

Tracking #:432316088

Date:25-07-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed several vulnerabilities, including a critical one, within LangChain, a popular open-source framework for generative AI.

TECHNICAL DETAILS:

Notable Vulnerabilities Details:

- **CVE-2023-44467** | Base Score: 9.8 - Critical | Prompt injection
    - Prompt injection in LangChain Experimental versions before 0.0.306, allowing arbitrary code execution via the PALChain feature.
- **CVE-2023-46229** | Base Score: 8.8 | High-Server-side request forgery (SSRF)
    - Server-side request forgery (SSRF) in versions earlier than 0.0.317 allows attackers to access internal APIs.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the latest version of LangChain AI.

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://unit42.paloaltonetworks.com/langchain-vulnerabilities/?web_view=true