مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

RCE Vulnerability in Ollama AI Platform

Tracking #:432315981

Date:25-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution (RCE) vulnerability in the Ollama open-source AI infrastructure platform.

TECHNICAL DETAILS:

A critical remote code execution (RCE) vulnerability (CVE-2024-37032, nicknamed "Probllama") observed in the Ollama open-source AI infrastructure platform and this flaw could allow an attacker to achieve full control over Ollama servers and compromise any AI models or applications hosted on them.

The vulnerability stems from insufficient input validation in the "/api/pull" API endpoint, which enables a path traversal attack. By providing a malicious model manifest file with a crafted payload, an attacker can overwrite arbitrary files on the server, including critical system configuration files. This can lead to remote code execution, especially in Docker deployments where the Ollama API server runs with root privileges.

Fixed Versions:

- Ollama 0.1.34 or Newer

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the affected versions to the fixed version released by Ollama at the earliest.

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-2024-37032