CVE-2024-21825 - Score: 8.8

Components:

ggerganov llama.cpp *

Description:

A heap-based buffer overflow vulnerability exists in the GGUF library GGUF_TYPE_ARRAY/GGUF_TYPE_STRING parsing functionality of llama.cpp Commit 18c2e17. A specially crafted .gguf file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.

Main problems:

190 "Integer Overflow or Wraparound"