# CVE Detail – CVE-2024-32878

Llama.cpp is LLM inference in C/C++. There is a use of uninitialized heap variable vulnerability in gguf\_init\_from\_file, the code will free this uninitialized variable later. In a simple POC, it will directly cause a crash. If the file is carefully constructed, it may be possible to control this uninitialized value and cause arbitrary address free problems. This may further lead to be exploited. Causes llama.cpp to crash (DoS) and may even lead to arbitrary code execution (RCE). This vulnerability has been patched in commit b2740.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.1943

## CVSS Scoring

CVSS v3.1 Score: 7.1

Severity: HIGH

## Mapped CWE(s)

* CWE-456: Missing Initialization of a Variable