



# llama.cpp has a Heap Buffer Overflow via Integer Overflow in GGUF Tensor Parsing

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-33298
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-24 01:17:01 UTC
<b>Updated</b>	2026-04-30 17:01:02 UTC
<b>Description</b>	llama.cpp is an inference of several LLM models in C/C++. Prior to b7824, an integer overflow vulnerability in the `ggml_nb`

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from security-advisories@github.com

**CVSS:** 3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**EPSS:** 0.000170000 probability, percentile 0.042940000 (date 2026-05-05)

**Problem Types:** CWE-122 | CWE-190 | CWE-122 CWE-122: Heap-based Buffer Overflow | CWE-190 CWE-190: Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ggml	Llama.cpp	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ggml-org	Llama.cpp	affected < b7824	Not specified

### References

Reference	Source	Link	Tags
github.com/ggml-org/llama.cpp/security/advisories/GHSA-96jg-mvhq-q7q7	security-advisories@github.com	github.com	Exploit, Vendor
github.com/ggml-org/llama.cpp/releases/tag/b7824	security-advisories@github.com	github.com	Release Notes
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)