



llama.cpp allows write-what-where in rpc_server::set_tensor

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

Summary

CVE	CVE-2024-42479
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-08-12 15:15:21 UTC
Updated	2026-04-27 17:44:53 UTC
Description	llama.cpp provides LLM inference in C/C++. The unsafe `data` pointer member in the `rpc_tensor` structure can cause arbitrary write-what-where.

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.056780000 probability, percentile 0.904140000 (date 2026-04-27)

Problem Types: CWE-123 | CWE-787 | CWE-123 CWE-123: Write-what-where Condition

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	security-advisories@github.com	Secondary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/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	Ggerganov	Llama.cpp	affected < b3561	Not specified
ADP	Ggerganov	Llama.cpp	affected b3561 custom	Not specified

References

Reference	Source	Link	Tags
github.com/ggerganov/llama.cpp/security/advisories/GHSA-wcr5-566p-9cwj	security-advisories@github.com	github.com	Exploit
github.com/ggerganov/llama.cpp/commit/b72942fac998672a79a1ae3c03b340f7e6...	security-advisories@github.com	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

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

CVE.report and Source URL Uptime Status status.cve.report