Ollama heap out-of-bounds read in GGUF tensor parsing leaks server process memory to unauthenticated remote attackers

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-7482
State	PUBLISHED
Assigner	Echo
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 13:16:01 UTC
Updated	2026-05-11 12:27:11 UTC
Description	Ollama before 0.17.1 contains a heap out-of-bounds read vulnerability in the GGUF model loader. The /api/create endpoint

Risk And Classification

Primary CVSS: v4.0 8.8 HIGH from abd028dc-c042-4c4d-9749-38d0f850af89

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:A/V:D/RE:L/U:Red

EPSS: 0.000990000 probability, percentile 0.271250000 (date 2026-05-11)

Problem Types: CWE-125 | CWE-125 CWE-125 Out-of-bounds Read

Version	Source	Type	Score	Severity	Vector
4.0	abd028dc-c042-4c4d-9749-38d0f850af89	Secondary	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA
4.0	CNA	CVSS	8.8	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA
3.1	abd028dc-c042-4c4d-9749-38d0f850af89	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
3.1	CNA	CVSS	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:Y/R:A/V:D/RE:L/U:Red

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Ollama	Ollama	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ollama	Ollama	affected 0.17.1 semver	Not specified

References

Reference	Source	Link
github.com/ollama/ollama/pull/14406	abd028dc-c042-4c4d-9749-38d0f850af89	github.com
github.com/ollama/ollama/commit/88d57d0483cca907e0b23a968c83627a20b21047	abd028dc-c042-4c4d-9749-38d0f850af89	github.com
github.com/ollama/ollama/releases/tag/v0.17.1	abd028dc-c042-4c4d-9749-38d0f850af89	github.com
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

Vendor Comments And Credit

Discovery Credit

CNA: Cyera Research Team (Dor Attias, Ofek Itach) (en)

Additional Advisory Data

Solutions

CNA: Upgrade to ollama 0.17.1 or later. The fix in PR #14406 validates that declared tensor offset+size do not exceed the GGUF file size before reading, and adds a length check in the quantizer prior to the unsafe read.

Workarounds

CNA: Until upgrade is possible: (1) ensure Ollama is bound to a trusted interface only (default OLLAMA_HOST=127.0.0.1); (2) front Ollama with a reverse proxy that requires authentication on /api/create and /api/push; (3) restrict outbound network egress from the Ollama host to prevent exfiltration via /api/push to attacker-controlled registries.

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

Free CVE JSON API cve.report/api

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