



vllm KV Block kv_cache_interface.py has_mamba_layers uninitialized resource

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

Summary

CVE	CVE-2026-7141
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-27 17:16:45 UTC
Updated	2026-05-01 20:30:23 UTC
Description	A vulnerability was found in vllm up to 0.19.0. The affected element is the function has_mamba_layers of the file vllm/v1/kv_

Risk And Classification

Primary CVSS: v4.0 2.9 LOW from cna@vulldb.com

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

EPSS: 0.000460000 probability, percentile 0.141440000 (date 2026-05-01)

Problem Types: CWE-908 | CWE-908 Uninitialized Resource

Version	Source	Type	Score	Severity	Vector
4.0	cna@vulldb.com	Secondary	2.9	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N/E:P
3.1	cna@vulldb.com	Primary	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	5.6	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
3.0	CNA	DECLARED	5.6	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
2.0	cna@vulldb.com	Secondary	5.1		AV:N/AC:H/Au:N/C:P/I:P/A:P
2.0	CNA	DECLARED	5.1		AV:N/AC:H/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

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

CVSS v3.0 Breakdown

Attack Vector

Network

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vllm	Vllm	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Vllm	affected 0.1	Not specified
CNA	Na	Vllm	affected 0.2	Not specified
CNA	Na	Vllm	affected 0.3	Not specified
CNA	Na	Vllm	affected 0.4	Not specified
CNA	Na	Vllm	affected 0.5	Not specified
CNA	Na	Vllm	affected 0.6	Not specified
CNA	Na	Vllm	affected 0.7	Not specified
CNA	Na	Vllm	affected 0.8	Not specified
CNA	Na	Vllm	affected 0.9	Not specified
CNA	Na	Vllm	affected 0.10	Not specified
CNA	Na	Vllm	affected 0.11	Not specified
CNA	Na	Vllm	affected 0.12	Not specified
CNA	Na	Vllm	affected 0.13	Not specified
CNA	Na	Vllm	affected 0.14	Not specified
CNA	Na	Vllm	affected 0.15	Not specified
CNA	Na	Vllm	affected 0.16	Not specified

CNA	Na	Vllm	affected 0.17	Not specified
CNA	Na	Vllm	affected 0.18	Not specified
CNA	Na	Vllm	affected 0.19.0	Not specified

References

Reference	Source	Link	Tags
github.com/AjAnubolu/vllm/commit/1ad67864c0c20f167929e64c875f5c28e1aad9fd	cna@vuldb.com	github.com	Patch
github.com/vllm-project/vllm/issues/39146	cna@vuldb.com	github.com	Issue Tracking
vuldb.com/vuln/359740	cna@vuldb.com	vuldb.com	Third Party Advisory,
github.com/vllm-project/vllm/issues/39146	cna@vuldb.com	github.com	Issue Tracking
vuldb.com/vuln/359740/cti	cna@vuldb.com	vuldb.com	Permissions Required
vuldb.com/submit/801297	cna@vuldb.com	vuldb.com	Third Party Advisory,
github.com/vllm-project/vllm/pull/39283	cna@vuldb.com	github.com	Issue Tracking, Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Zyz3366 (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-04-26T00:00:00.000Z	Advisory disclosed
CNA	2026-04-26T02:00:00.000Z	VulDB entry created
CNA	2026-04-26T21:43:06.000Z	VulDB entry last update

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](#)