人工智能重要漏洞通报

（2026 年第十五期）

根据国家人工智能安全漏洞库（AIVD）统计，近期（2026 年 9 月 29 日至 2026 年 10 月 30 日）共采集重要人工智能漏洞 363 个，AIVD 对这些漏洞进行了收录。本周人工智能类漏洞主要涵盖了 DeepSeek、Ollama、MLflow 等多个厂商（项目）。AIVD 对其危害等级进行了评价，其中超危漏洞 41 个，高危漏洞 182 个，中危漏洞 140 个。

（一）人工智能漏洞增长数量情况

近期 AIVD 采集人工智能漏洞 363 个。

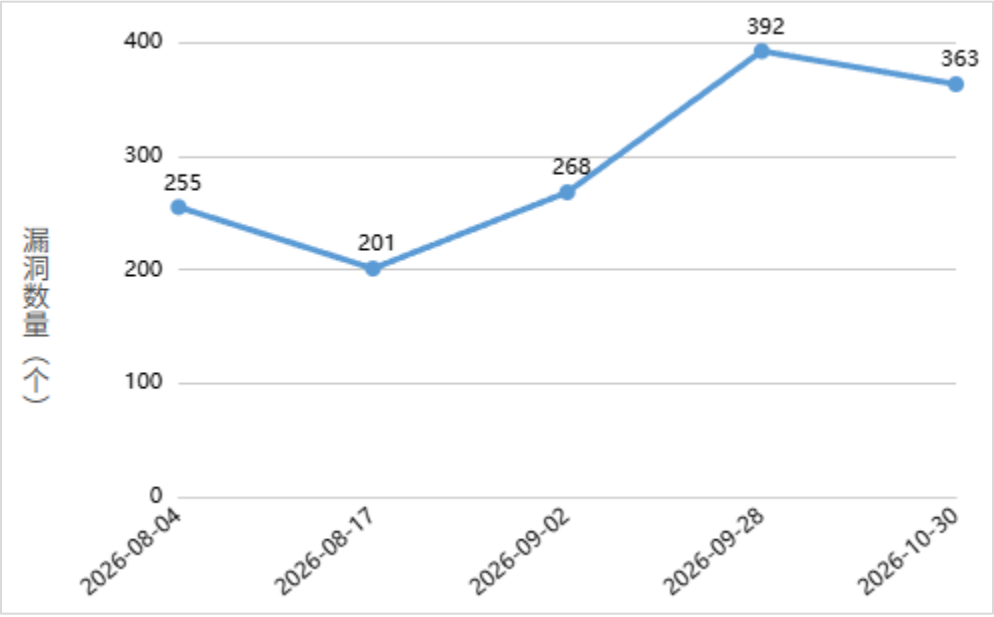


图 1 近五周漏洞新增数量统计图

（二）人工智能漏洞具体情况

近期共采集重要人工智能漏洞 363 个，包括 DeepSeek、Ollama、MLflow 等多个厂商（项目）的漏洞。其中超危漏洞 41 个，高危漏洞 182 个，中危漏洞 140 个。具体如表 1 所示：

表 1 人工智能漏洞列表

序号	漏洞名称	CNNVD 编号	CVE 编号	危害等级	参考链接	厂商（项目）
1	AgentScope-AI agentscope 代码注入漏洞	CNNVD-2026-96542691	CVE-2026-51856	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	AgentScope-AI
2	Agno 代码注入漏洞	CNNVD-2026-21068400	CVE-2026-119050	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Agno
3	Amazon sagemaker-python-sdk 授权问题漏洞	CNNVD-2026-61426883	CVE-2026-112408	超危	https://github.com/aws/sagemaker-python-sdk/security/advisories/GHSA-5rx8-8fr2-f855	Amazon
4	Carmine Paolino ruby_llm 安全漏洞	CNNVD-2026-56463895	CVE-2026-67989	超危	https://github.com/crmne/ruby_llm/commit/dd3c84812598def03d4aff77b	Carmine Paolino

					5447c41d8f5c34e	
5	Chatchat-Space Langchain-Chatchat 授权问题漏洞	CNNVD-2026-13673042	CVE-2026-75128	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Chatchat-Space
6	DeepSeek 信息泄露漏洞	CNNVD-2026-41538350	CVE-2026-52394	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	DeepSeek
7	eosphoros DB-GPT 路径遍历漏洞	CNNVD-2026-70521096	CVE-2026-51864	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	eosphoros
8	eosphoros DB-GPT 代码注入漏洞	CNNVD-2026-83885455	CVE-2026-51866	超危	https://github.com/eosphoros-ai/DB-GPT/issues/3047	eosphoros
9	eosphoros DB-GPT 信任管理问题漏洞	CNNVD-2026-86904884	CVE-2026-77933	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户	eosphoros

					随时关注厂商主页或参考网址以获取解决办法。	
10	eosphoros DB-GPT 授权问题漏洞	CNNVD-2026-96185061	CVE-2026-77932	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	eosphoros
11	Ettore Di Giacinto LocalAI 服务端请求伪造漏洞	CNNVD-2026-81794055	CVE-2026-114493	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Ettore Di Giacinto
12	ggml llama.cpp 缓冲区错误漏洞	CNNVD-2026-77337808	CVE-2026-118375	超危	https://github.com/ggml-org/llama.cpp/commit/9a0fde9967fa1a35b6e5dd1f47e1a3648b6fecc1,https://github.com/ggml-org/llama.cpp/releases/tag/b11865	ggml
13	ggml llama.cpp 资源管理错误漏洞	CNNVD-2026-24411958	CVE-2026-107183	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户	ggml

					随时关注厂商主页或参考网址以获取解决办法。	
14	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-57928666	CVE-2026-104339	超危	https://www.ibm.com/support/pages/node/7293015	IBM
15	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-13430166	CVE-2026-93680	超危	https://www.ibm.com/support/pages/node/7294467	IBM
16	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-73253135	CVE-2026-93674	超危	https://www.ibm.com/support/pages/node/7290694	IBM
17	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-22767753	CVE-2026-110186	超危	https://www.ibm.com/support/pages/node/7294467	IBM
18	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-98182337	CVE-2026-107329	超危	https://www.ibm.com/support/pages/node/7293016	IBM
19	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-24793642	CVE-2026-107328	超危	https://www.ibm.com/support/pages/node/7293016	IBM
20	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-34146358	CVE-2026-107327	超危	https://www.ibm.com/support/pages/node/7293016	IBM
21	iFLYTEK Astron Agent 信任管理问题漏洞	CNNVD-2026-73530802	CVE-2026-108263	超危	https://github.com/iflytek/astron-agent	iFLYTEK
22	LMCache 授权问题漏洞	CNNVD-2026-16764200	CVE-2026-105192	超危	https://github.com/LMCache/LMCach	LMCache

					e/releases	
23	LMCache 授权问题漏洞	CNNVD-2026-81558846	CVE-2026-107204	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	LMCache
24	Mage OSS 异常处理不当漏洞	CNNVD-2026-32072180	CVE-2026-111823	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Mage
25	Martin Legrand AgenticSeek 调试信息泄露漏洞	CNNVD-2026-35113430	CVE-2026-115727	超危	https://github.com/Fosowl/agenticSeek/commit/409840c033851d861c5c83a91c05fd4a2a75a096	Martin Legrand
26	Mem0 SQL 注入漏洞	CNNVD-2026-33052244	CVE-2026-115324	超危	https://github.com/mem0ai/mem0/commit/a2ffca32660537b7b304305f36774ae2a13452cb,https://github.com/mem0ai/mem0/releases/tag/v1.0.8	Mem0
27	Mervin Praison PraisonAI 信息泄露漏洞	CNNVD-2026-57718543	CVE-2026-57116	超危	https://github.com/MervinPraison/PraisonAI/s	Mervin Praison

					ecurity/advisories/GHSA-892r-p3jq-jp24	
28	Mervin Praison PraisonAI 代码注入漏洞	CNNVD-2026-51879550	CVE-2026-62176	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Mervin Praison
29	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-49044595	CVE-2026-57118	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-x8cv-xmq7-p8xp	Mervin Praison
30	MLflow 代码注入漏洞	CNNVD-2026-97129426	CVE-2026-116692	超危	https://github.com/mlflow/mlflow/security/advisories/GHSA-26p8-2jq9-3vq9	MLflow
31	ogx-ai OGX 安全漏洞	CNNVD-2026-27940171	CVE-2026-77177	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	ogx-ai
32	Ollama 路径遍历漏洞	CNNVD-2026-80790656	CVE-2026-103663	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户	Ollama

					随时关注厂商主页或参考网址以获取解决办法。	
33	Red Hat OpenShift AI 授权问题漏洞	CNNVD-2026-60522897	CVE-2026-117574	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Red Hat
34	RVC-Boss GPT-SoVITS-WebUI 命令注入漏洞	CNNVD-2026-20730235	CVE-2025-71429	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	RVC-Boss
35	ServiceNow AI Platform 权限许可和访问控制问题漏洞	CNNVD-2026-88386239	CVE-2026-103093	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	ServiceNow
36	ServiceNow AI Platform 安全漏洞	CNNVD-2026-94348552	CVE-2026-13016	超危	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3159623	ServiceNow
37	ServiceNow AI	CNNVD-2026-	CVE-2026-	超危	https://sup	ServiceNo

	Platform 授权问题漏洞	23405888	86860		port.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3159623	w
38	sgl-project SGLang 反序列化注入漏洞	CNNVD-2026-90305414	CVE-2026-93034	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	sgl-project
39	sgl-project SGLang 代码注入漏洞	CNNVD-2026-49693750	CVE-2026-111391	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	sgl-project
40	Tuğcan Topaloğlu OpenClaw Agent Dashboard 跨站脚本漏洞	CNNVD-2026-28013068	CVE-2026-66418	超危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Tuğcan Topaloğlu
41	vLLM 代码注入漏洞	CNNVD-2026-59941489	CVE-2026-114053	超危	https://github.com/vllm-project/vllm/security/advisories/GHSA-h3rc-	vLLM

					6mm3-gc2m	
42	Agent Zero 跨站脚本漏洞	CNNVD-2026-43352219	CVE-2026-97635	高危	https://github.com/agent0ai/agent-zero/releases/tag/v1.15	Agent Zero
43	Agent Zero 路径遍历漏洞	CNNVD-2026-61273318	CVE-2026-51853	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Agent Zero
44	Aider AI aider 命令注入漏洞	CNNVD-2026-92631431	CVE-2026-115726	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Aider AI
45	Amazon GluonTS 代码注入漏洞	CNNVD-2026-47804627	CVE-2026-100308	高危	https://github.com/awslabs/gluonts/security/advisories/GHSA-64q6-5qv7-cwj9	Amazon
46	AMD ROCm Communication Collectives Library 缓冲区错误漏洞	CNNVD-2026-99628927	CVE-2026-43598	高危	https://www.amd.com/en/resources/product-security/bulletin/AMD-SB-6033.html	AMD
47	BentoML 命令注入漏洞	CNNVD-2026-83540327	CVE-2026-112264	高危	目前厂商暂未发布修复	BentoML

					措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
48	coze-dev coze-studio 授权问题漏洞	CNNVD-2026-62737776	CVE-2026-77935	高危	https://www.lasso.security/vulnerability-database/cve-2026-77935	coze-dev
49	coze-dev coze-studio 配置错误漏洞	CNNVD-2026-11032676	CVE-2026-77934	高危	https://github.com/coze-dev/coze-studio/commit/fcf40d1008c100108c23be051a49950283f2c2cf	coze-dev
50	CrewAI AMP Suite 服务端请求伪造漏洞	CNNVD-2026-13937340	CVE-2026-112308	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	crewAI
51	CrewAI AMP Suite 代码注入漏洞	CNNVD-2026-23694459	CVE-2026-92206	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	CrewAI
52	decolua	CNNVD-2026-	CVE-2026-	高危	目前厂商暂	decolua

	9Router 代码注入漏洞	77548935	108593		未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
53	Eric Buehler mistral.rs 后置链接漏洞	CNNVD-2026-73902461	CVE-2026-108759	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Eric Buehler
54	Flyte 加密问题漏洞	CNNVD-2026-53272774	CVE-2026-108728	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Flyte
55	Flyto2 Core 授权问题漏洞	CNNVD-2026-32076929	CVE-2026-55786	高危	https://github.com/flytohub/flyto-core/security/advisories/GHSA-h9f9-h6gm-wc85	Flyto2
56	Flyto2 Core 服务端请求伪造漏洞	CNNVD-2026-21102565	CVE-2026-55787	高危	https://github.com/flytohub/flyto-core/security/advisori	Flyto2

					es/GHSA-794r-5rp2-fpg8	
57	ggml llama.cpp 输入验证错误漏洞	CNNVD-2026-23329354	CVE-2026-116816	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	ggml
58	ggml llama.cpp 异常处理不当漏洞	CNNVD-2026-73602738	CVE-2026-119052	高危	https://github.com/ggml-org/llama.cpp/commit/7ecb57f7adbea2928aa468ad2aecf05b10725ad4,https://github.com/ggml-org/llama.cpp/releases/tag/b11935	ggml
59	Hugging Face Datasets 反序列化注入漏洞	CNNVD-2026-35537648	CVE-2026-57845	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Hugging Face
60	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-43509499	CVE-2026-104328	高危	https://www.ibm.com/support/pages/node/7293015	IBM
61	IBM Langflow OSS 反序列化注入漏洞	CNNVD-2026-90209828	CVE-2026-104317	高危	https://www.ibm.com/support/pages	IBM

					/node/7293015	
62	IBM Langflow OSS 反序列化注入漏洞	CNNVD-2026-28330280	CVE-2026-104324	高危	https://www.ibm.com/support/pages/node/7293015	IBM
63	IBM Langflow OSS 权限许可和访问控制问题漏洞	CNNVD-2026-83794221	CVE-2026-103092	高危	https://www.ibm.com/support/pages/node/7293015	IBM
64	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-71851333	CVE-2026-101288	高危	https://www.ibm.com/support/pages/node/7293015	IBM
65	IBM Planning Analytics 缓冲区错误漏洞	CNNVD-2026-72223500	CVE-2026-76587	高危	https://www.ibm.com/support/pages/node/7291604	IBM
66	IBM Planning Analytics 缓冲区错误漏洞	CNNVD-2026-38028772	CVE-2026-85457	高危	https://www.ibm.com/support/pages/node/7291604	IBM
67	IBM Langflow OSS 权限许可和访问控制问题漏洞	CNNVD-2026-72145375	CVE-2026-97680	高危	https://www.ibm.com/support/pages/node/7290694	IBM
68	IBM Langflow OSS 处理逻辑错误漏洞	CNNVD-2026-66880431	CVE-2026-97678	高危	https://www.ibm.com/support/pages/node/7290694	IBM
69	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-51649186	CVE-2026-97679	高危	https://www.ibm.com/support/pages/node/7290694	IBM
70	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-91497092	CVE-2026-97676	高危	https://www.ibm.com/support/pages/node/7290694	IBM

71	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-34415300	CVE-2026-97674	高危	https://www.ibm.com/support/pages/node/7290694	IBM
72	IBM Langflow OSS 处理逻辑错误漏洞	CNNVD-2026-91094557	CVE-2026-97673	高危	https://www.ibm.com/support/pages/node/7290694	IBM
73	IBM Planning Analytics 路径遍历漏洞	CNNVD-2026-57905400	CVE-2026-75061	高危	https://www.ibm.com/support/pages/node/7291604	IBM
74	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-75462158	CVE-2026-97655	高危	https://www.ibm.com/support/pages/node/7290694	IBM
75	IBM Planning Analytics 路径遍历漏洞	CNNVD-2026-55253110	CVE-2026-19627	高危	https://www.ibm.com/support/pages/node/7291604	IBM
76	IBM Planning Analytics 授权问题漏洞	CNNVD-2026-89740004	CVE-2026-19622	高危	https://www.ibm.com/support/pages/node/7291604	IBM
77	IBM Planning Analytics 授权问题漏洞	CNNVD-2026-65173615	CVE-2026-19620	高危	https://www.ibm.com/support/pages/node/7291604	IBM
78	IBM Planning Analytics 授权问题漏洞	CNNVD-2026-13479297	CVE-2026-17475	高危	https://www.ibm.com/support/pages/node/7291604	IBM
79	IBM Langflow OSS 处理逻辑错误漏洞	CNNVD-2026-47389833	CVE-2026-93675	高危	https://www.ibm.com/support/pages/node/7290694	IBM
80	IBM Langflow OSS 授权问题漏	CNNVD-2026-28245007	CVE-2026-93678	高危	https://www.ibm.com/su	IBM

	洞				pport/pages/node/7290694	
81	IBM Langflow OSS 信息泄露漏洞	CNNVD-2026-41055095	CVE-2026-93677	高危	https://www.ibm.com/support/pages/node/7290694	IBM
82	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-86121017	CVE-2026-93449	高危	https://www.ibm.com/support/pages/node/7290694	IBM
83	IBM Langflow OSS 反序列化注入漏洞	CNNVD-2026-64602142	CVE-2026-93447	高危	https://www.ibm.com/support/pages/node/7290694	IBM
84	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-79447788	CVE-2026-93445	高危	https://www.ibm.com/support/pages/node/7290694	IBM
85	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-95425188	CVE-2026-93443	高危	https://www.ibm.com/support/pages/node/7290694	IBM
86	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-18175044	CVE-2026-110245	高危	https://www.ibm.com/support/pages/node/7293016	IBM
87	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-82267833	CVE-2026-110309	高危	https://www.ibm.com/support/pages/node/7293016	IBM
88	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-96143289	CVE-2026-110244	高危	https://www.ibm.com/support/pages/node/7293016	IBM
89	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-82491097	CVE-2026-110196	高危	https://www.ibm.com/support/pages/node/72930	IBM

					16	
90	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-44197018	CVE-2026-110193	高危	https://www.ibm.com/support/pages/node/7294467	IBM
91	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-23533372	CVE-2026-88962	高危	https://www.ibm.com/support/pages/node/7290694	IBM
92	IBM Langflow OSS 命令注入漏洞	CNNVD-2026-23470033	CVE-2026-107326	高危	https://www.ibm.com/support/pages/node/7293016	IBM
93	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-23833645	CVE-2026-107366	高危	https://www.ibm.com/support/pages/node/7293016	IBM
94	JetBrains Junie CLI 软件供应链问题漏洞	CNNVD-2026-16298552	CVE-2026-111091	高危	https://www.jetbrains.com/privacy-security/issues-fixed/	JetBrains
95	JetBrains datalore 路径遍历漏洞	CNNVD-2026-46350788	CVE-2026-111093	高危	https://www.jetbrains.com/privacy-security/issues-fixed/	JetBrains
96	Jovan Marinovic Network-AI 处理逻辑错误漏洞	CNNVD-2026-88318263	CVE-2026-109331	高危	https://github.com/Jovancoding/Network-AI/security/advisories/GHSA-9p2w-prp8-5722	Jovan Marinovic
97	kuafuai aipexbase SQL 注入漏洞	CNNVD-2026-13914029	CVE-2026-111718	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户	kuafuai

					随时关注厂商主页或参考网址以获取解决办法。	
98	Kubeflow Hub 服务端请求伪造漏洞	CNNVD-2026-52153143	CVE-2026-110220	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Kubeflow
99	kvcache.ai Mooncake 授权问题漏洞	CNNVD-2026-93402415	CVE-2026-106040	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	kvcache.ai
100	LangBot 输入验证错误漏洞	CNNVD-2026-17190517	CVE-2026-112265	高危	https://github.com/langbot-app/LangBot/commit/43c481d74a6388657b84baa7d292c613c75c24f9	LangBot
101	LangChain LangGraph 授权问题漏洞	CNNVD-2026-92610412	CVE-2026-104873	高危	https://github.com/langchain-ai/langgraph/security/advisories/GHSA-fvww-7h3r-vfhp	LangChain
102	LlamaFarm 配置错误漏洞	CNNVD-2026-62130363	CVE-2026-108760	高危	目前厂商暂未发布修复措施解决此	Llama Farm

					安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
103	LMCache 授权问题漏洞	CNNVD-2026-92318089	CVE-2026-107206	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	LMCache
104	LMCache 授权问题漏洞	CNNVD-2026-28065481	CVE-2026-107205	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	LMCache
105	Massimiliano Pippi banks 路径遍历漏洞	CNNVD-2026-51930673	CVE-2026-107716	高危	https://github.com/masci/banks/security/advisories/GHSA-556j-vv39-8rqv	Massimiliano Pippi
106	Mervin Praison PraisonAI 信息泄露漏洞	CNNVD-2026-66118661	CVE-2026-57146	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-jxcw-qp4h-6jfq	Mervin Praison
107	Mervin Praison PraisonAI 权限	CNNVD-2026-85269180	CVE-2026-57144	高危	https://github.com/Mer	Mervin Praison

	许可和访问控制问题漏洞				vinPraison/PraisonAI/security/advisories/GHSA-6jcq-6546-qrrw	
108	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-39861867	CVE-2026-57121	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-rh39-9c67-59mh	Mervin Praison
109	Mervin Praison PraisonAI 命令注入漏洞	CNNVD-2026-19069872	CVE-2026-57142	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-7qw2-w5rc-37x2	Mervin Praison
110	Mervin Praison PraisonAI 竞争条件问题漏洞	CNNVD-2026-21382325	CVE-2026-57114	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-rjvw-7vvw-549v	Mervin Praison
111	Mervin Praison PraisonAI 路径遍历漏洞	CNNVD-2026-54847892	CVE-2026-57113	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-f44v-7qgw-9gh9	Mervin Praison
112	Mervin Praison PraisonAI 命令注入漏洞	CNNVD-2026-55741921	CVE-2026-57117	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-w6h2-fr4q-xvxv	Mervin Praison
113	Mervin Praison	CNNVD-2026-	CVE-2026-	高危	https://git	Mervin

	PraisonAI 跨站脚本漏洞	35935302	56840		hub.com/MervinPraison/PraisonAI/security/advisories/GHSA-63v4-w882-g4x2	Praison
114	Mervin Praison PraisonAI 处理逻辑错误漏洞	CNNVD-2026-60025077	CVE-2026-56838	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-v847-hxxw-3pxg	Mervin Praison
115	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-49200525	CVE-2026-56837	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-fc26-m9pf-v56q	Mervin Praison
116	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-24929115	CVE-2026-56836	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-5qw8-f2g9-ff29	Mervin Praison
117	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-74520558	CVE-2026-56835	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-qvpf-j64c-jmhr	Mervin Praison
118	Mervin Praison PraisonAI 信息泄露漏洞	CNNVD-2026-63556613	CVE-2026-56834	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-j7qx-p75m-wp7g	Mervin Praison

119	Mervin Praison PraisonAI 信息泄露漏洞	CNNVD-2026-31319011	CVE-2026-56833	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-22cj-m4wf-fv2c	Mervin Praison
120	Mervin Praison PraisonAI 输入验证错误漏洞	CNNVD-2026-72936633	CVE-2026-56832	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-8579-rgg5-ph2m	Mervin Praison
121	Mervin Praison PraisonAI 输入验证错误漏洞	CNNVD-2026-64890438	CVE-2026-57143	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-4pcv-mg8v-vrgf	Mervin Praison
122	Microsoft Azure AI Foundry 服务端请求伪造漏洞	CNNVD-2026-59665177	CVE-2026-108456	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108456	Microsoft
123	MindsDB 代码注入漏洞	CNNVD-2026-14494476	CVE-2026-92207	高危	https://github.com/mindsdb/mindshub/releases	MindsDB
124	Mistral AI Mistral Vibe 处理逻辑错误漏洞	CNNVD-2026-85422504	CVE-2026-109429	高危	https://github.com/mistralai/mistral-vibe/releases/tag/v2.25.4	Mistral AI
125	Mistral AI Mistral Vibe 处理逻辑错误漏洞	CNNVD-2026-14375059	CVE-2026-109428	高危	https://github.com/mistralai/mistral-	Mistral AI

					vibe/releases/tag/v2.25.5	
126	MLflow 路径遍历漏洞	CNNVD-2026-47957681	CVE-2026-116690	高危	https://github.com/mlflow/mlflow/security/advisories/GHSA-m65p-9j7q-6w33	MLflow
127	MLflow 路径遍历漏洞	CNNVD-2026-66396787	CVE-2026-53995	高危	https://github.com/SaiTeja-Erukude/CVE-2026-53995-mlflow-path-traversal	MLflow
128	ModelScope AgentScope 路径遍历漏洞	CNNVD-2026-11033299	CVE-2026-51568	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	ModelScope
129	ModelScope AgentScope 安全漏洞	CNNVD-2026-86929672	CVE-2026-51570	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	ModelScope
130	ModelTC LightLLM 反序列化注入漏洞	CNNVD-2026-46177777	CVE-2026-111160	高危	https://github.com/ModelTC/LightLLM/issues/1629	ModelTC
131	Natural	CNNVD-2026-	CVE-2026-	高危	https://git	Natural

	Language Toolkit 路径遍历漏洞	31573228	109956		hub.com/nltk/nltk/security/advisories/GHSA-j456-xh4h-cpf2	Language Toolkit
132	ntop nDPI 数字错误漏洞	CNNVD-2026-13256956	CVE-2026-88357	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	ntop
133	NVIDIA virtual gpu manager 权限许可和访问控制问题漏洞	CNNVD-2026-27018804	CVE-2026-47574	高危	https://www.nvidia.com/en-us/security/	NVIDIA
134	NVIDIA virtual gpu manager 缓冲区错误漏洞	CNNVD-2026-51710665	CVE-2026-47541	高危	https://www.nvidia.com/en-us/security/	NVIDIA
135	NVIDIA virtual gpu manager 缓冲区错误漏洞	CNNVD-2026-70896051	CVE-2026-47536	高危	https://www.nvidia.com/en-us/security/	NVIDIA
136	NVIDIA virtual gpu manager 缓冲区错误漏洞	CNNVD-2026-34471232	CVE-2026-47535	高危	https://www.nvidia.com/en-us/security/	NVIDIA
137	NVIDIA virtual gpu manager 缓冲区错误漏洞	CNNVD-2026-93006694	CVE-2026-47521	高危	https://www.nvidia.com/en-us/security/	NVIDIA
138	NVIDIA virtual gpu manager 缓冲区错误漏洞	CNNVD-2026-12560082	CVE-2026-47503	高危	https://www.nvidia.com/en-us/security/	NVIDIA

139	NVIDIA virtual gpu manager 缓冲区错误漏洞	CNNVD-2026-97098453	CVE-2026-47499	高危	https://www.nvidia.com/en-us/security/	NVIDIA
140	NVIDIA virtual gpu manager 缓冲区错误漏洞	CNNVD-2026-73397894	CVE-2026-47496	高危	https://www.nvidia.com/en-us/security/	NVIDIA
141	NVIDIA virtual gpu manager 缓冲区错误漏洞	CNNVD-2026-89663287	CVE-2026-47498	高危	https://www.nvidia.com/en-us/security/	NVIDIA
142	NVIDIA virtual gpu manager 竞争条件问题漏洞	CNNVD-2026-52320695	CVE-2026-47497	高危	https://www.nvidia.com/en-us/security/	NVIDIA
143	NVIDIA virtual gpu manager 缓冲区错误漏洞	CNNVD-2026-14194348	CVE-2026-47495	高危	https://www.nvidia.com/en-us/security/	NVIDIA
144	NVIDIA virtual gpu manager 授权问题漏洞	CNNVD-2026-56641057	CVE-2026-47493	高危	https://www.nvidia.com/en-us/security/	NVIDIA
145	NVIDIA megatron-lm 反序列化注入漏洞	CNNVD-2026-29485992	CVE-2026-65180	高危	https://www.nvidia.com/en-us/security/	NVIDIA
146	NVIDIA isaac lab 代码注入漏洞	CNNVD-2026-56812481	CVE-2026-65141	高危	https://www.nvidia.com/en-us/security/	NVIDIA
147	NVIDIA megatron-lm 反序列化注入漏洞	CNNVD-2026-54058322	CVE-2026-65110	高危	https://www.nvidia.com/en-us/security/	NVIDIA
148	NVIDIA megatron-lm 加	CNNVD-2026-16865858	CVE-2026-65104	高危	https://www.nvidia.com	NVIDIA

	密问题漏洞				/en-us/security/	
149	Obot AI Obot 授权问题漏洞	CNNVD-2026-83649762	CVE-2026-103758	高危	https://github.com/obot-platform/obot/security/advisories/GHSA-6fwv-3h4c-37j9	Obot AI
150	Obot AI Obot 跨站请求伪造漏洞	CNNVD-2026-66473558	CVE-2026-114662	高危	https://github.com/obot-platform/obot/security/advisories/GHSA-2qcm-3gv6-2mfc	Obot AI
151	Obot AI Obot 信任管理问题漏洞	CNNVD-2026-62101954	CVE-2026-105138	高危	https://github.com/obot-platform/obot/security/advisories/GHSA-q5wf-87f5-cxgq	Obot AI
152	Ollama 授权问题漏洞	CNNVD-2026-58859990	CVE-2026-102697	高危	https://github.com/ollama/ollama/releases/tag/v0.31.2	Ollama
153	Omnigent 路径遍历漏洞	CNNVD-2026-58610379	CVE-2026-112015	高危	https://github.com/omnigent-ai/omnigent/security/advisories/GHSA-p5x3-3gqh-x44g	omnigent
154	openagents-org openagents 授权问题漏洞	CNNVD-2026-68116347	CVE-2026-108739	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂	openagents-org

					商主页或参考网址以获取解决办法。	
155	OpenStack Mistral 授权问题漏洞	CNNVD-2026-18215168	CVE-2026-97147	高危	https://security.openstack.org/ossa/OSSA-2026-044.html	OpenStack
156	OpenStack Mistral 授权问题漏洞	CNNVD-2026-17098537	CVE-2026-93860	高危	https://security.openstack.org/ossa/OSSA-2026-044.html	OpenStack
157	OpenStack Mistral 命令注入漏洞	CNNVD-2026-20058458	CVE-2026-93858	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	OpenStack
158	Oraios AI Serena 后置链接漏洞	CNNVD-2026-30817042	CVE-2026-109965	高危	https://github.com/oraios/serena/commit/6f20f9b822d85bb063008e786f808d04619dd54e	Oraios AI
159	Project MONAI MONAI 代码注入漏洞	CNNVD-2026-97856917	CVE-2026-118683	高危	https://github.com/Project-MONAI/MONAI/security/advisories/GHSA-wvpx-5qmp-46g3	Project MONAI
160	Project MONAI MONAI 加密问题漏洞	CNNVD-2026-50217135	CVE-2026-118684	高危	https://github.com/Project-MONAI/MONAI	Project MONAI

					/security/advisories/GHSA-hhh4-h52m-fqh6	
161	Project MONAI MONAI 反序列化注入漏洞	CNNVD-2026-65287277	CVE-2026-109361	高危	https://github.com/Project-MONAI/MONAI/security/advisories/GHSA-8f32-8649-rv87	Project MONAI
162	Project MONAI MONAI 反序列化注入漏洞	CNNVD-2026-56519384	CVE-2026-109360	高危	https://github.com/Project-MONAI/MONAI/security/advisories/GHSA-vm9c-7j6g-c7mm	Project MONAI
163	Pydantic pydantic-ai 跨站请求伪造漏洞	CNNVD-2026-76104090	CVE-2026-107295	高危	https://github.com/pydantic/pydantic-ai/releases	Pydantic
164	Pydantic pydantic-ai 资源管理错误漏洞	CNNVD-2026-36697507	CVE-2026-107286	高危	https://github.com/pydantic/pydantic-ai/security/advisories/GHSA-6fqq-452j-qhrp	Pydantic
165	Red Hat OpenShift AI 服务端请求伪造漏洞	CNNVD-2026-65697139	CVE-2026-13451	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Red Hat
166	Roomote Roo Code 处理逻辑错误漏洞	CNNVD-2026-10067068	CVE-2026-110206	高危	目前厂商暂未发布修复措施解决此	Roomote

					安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
167	Roomote Roo Code 输入验证错误漏洞	CNNVD-2026-97111404	CVE-2026-110205	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Roomote
168	Roomote Roo Code 处理逻辑错误漏洞	CNNVD-2026-99795678	CVE-2026-110204	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Roomote
169	Roomote Roo Code 处理逻辑错误漏洞	CNNVD-2026-29953015	CVE-2026-110203	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Roomote
170	Roomote Roo Code 处理逻辑错误漏洞	CNNVD-2026-95155453	CVE-2026-110202	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户	Roomote

					随时关注厂商主页或参考网址以获取解决办法。	
171	SAMSUNG Bixby 输入验证错误漏洞	CNNVD-2026-44533132	CVE-2026-21157	高危	https://security.samsungmobile.com/serviceWeb.smsb?year=2026&month=07	SAMSUNG
172	ServiceNow AI Platform 安全漏洞	CNNVD-2026-58112363	CVE-2026-103094	高危	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3228994	ServiceNow
173	ServiceNow AI Platform 权限许可和访问控制问题漏洞	CNNVD-2026-78303210	CVE-2026-86858	高危	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3159623	ServiceNow
174	ServiceNow AI Platform 权限许可和访问控制问题漏洞	CNNVD-2026-58237688	CVE-2026-86859	高危	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3159623	ServiceNow
175	ServiceNow AI Platform 授权问题漏洞	CNNVD-2026-84071087	CVE-2026-86857	高危	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3159623	ServiceNow
176	sgl-project SGLang 资源管理错误漏洞	CNNVD-2026-55699613	CVE-2026-112270	高危	目前厂商暂未发布修复措施解决此	sgl-project

					安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
177	sgl-project SGLang 资源管理错误漏洞	CNNVD-2026-35685617	CVE-2026-112269	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	sgl-project
178	sgl-project SGLang 输入验证错误漏洞	CNNVD-2026-92382609	CVE-2026-112266	高危	https://github.com/sgl-project/sglang/releases	sgl-project
179	sgl-project sglang 处理逻辑错误漏洞	CNNVD-2026-71493591	CVE-2026-102634	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	sgl-project
180	sgl-project SGLang 资源管理错误漏洞	CNNVD-2026-30513514	CVE-2026-109229	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	sgl-project

181	sgl-project SGLang 资源管理错误漏洞	CNNVD-2026-79142110	CVE-2026-109228	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	sgl-project
182	sgl-project SGLang 资源管理错误漏洞	CNNVD-2026-87251147	CVE-2026-109227	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	sgl-project
183	sgl-project SGLang 资源管理错误漏洞	CNNVD-2026-14353951	CVE-2026-109226	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	sgl-project
184	sgl-project SGLang 资源管理错误漏洞	CNNVD-2026-42989015	CVE-2026-109225	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	sgl-project
185	sgl-project SGLang 资源管理错误漏洞	CNNVD-2026-25801514	CVE-2026-112082	高危	https://github.com/sgl-	sgl-project

					project/sglang/releases	
186	SillyTavern 资源管理错误漏洞	CNNVD-2026-50514053	CVE-2026-108545	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	SillyTavern
187	Tuğcan Topaloğlu OpenClaw Agent Dashboard 跨站脚本漏洞	CNNVD-2026-42242300	CVE-2026-66421	高危	https://github.com/tugcantopaloglu/openclaw-dashboard/releases	Tuğcan Topaloğlu
188	Ultralytics 路径遍历漏洞	CNNVD-2026-42015776	CVE-2026-118619	高危	https://github.com/ultralytics/ultralytics/releases	ultralytics
189	Ultralytics 代码注入漏洞	CNNVD-2026-73369798	CVE-2026-118618	高危	https://github.com/ultralytics/ultralytics/releases	ultralytics
190	Ultralytics 代码注入漏洞	CNNVD-2026-34143122	CVE-2026-118614	高危	https://github.com/ultralytics/ultralytics/releases	ultralytics
191	Ultralytics 代码注入漏洞	CNNVD-2026-17539048	CVE-2026-118616	高危	https://github.com/ultralytics/ultralytics/releases	ultralytics
192	Ultralytics 反序列化注入漏洞	CNNVD-2026-11768182	CVE-2026-118617	高危	https://github.com/ultralytics/ultralytics/releases	ultralytics
193	Ultralytics 命令注入漏洞	CNNVD-2026-44251267	CVE-2026-118615	高危	https://github.com/ult	ultralytics

					ralytics/ultralytics/releases	
194	Ultralytics 反序列化注入漏洞	CNNVD-2026-31830208	CVE-2026-118613	高危	https://github.com/ultralytics/ultralytics/releases	ultralytics
195	UnicomAI Wanwu 授权问题漏洞	CNNVD-2026-82598016	CVE-2026-108853	高危	https://github.com/UnicomAI/wanwu/releases	UnicomAI
196	vLLM 输入验证错误漏洞	CNNVD-2026-70024242	CVE-2026-115915	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-h3rc-j82p-2c3h	vLLM
197	vLLM 反序列化注入漏洞	CNNVD-2026-35105129	CVE-2026-115912	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-6757-hggm-hp2w	vLLM
198	vLLM 输入验证错误漏洞	CNNVD-2026-18862311	CVE-2026-109311	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-m52c-39rh-f3gp	vLLM
199	vLLM 输入验证错误漏洞	CNNVD-2026-91327345	CVE-2026-116181	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-w9r6-29q4-pvpr	vLLM
200	vLLM 资源管理错误漏洞	CNNVD-2026-92917856	CVE-2026-116179	高危	https://github.com/vllm-	vLLM

					project/vllm/security/advisories/GHSA-4m6g-h9mv-wqjc	
201	vLLM 资源管理错误漏洞	CNNVD-2026-61186821	CVE-2026-116177	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-mm38-5g96-7j6x	vLLM
202	vLLM 输入验证错误漏洞	CNNVD-2026-19565584	CVE-2026-116178	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-34qw-q2h2-jp3m	vLLM
203	vLLM 资源管理错误漏洞	CNNVD-2026-92326093	CVE-2026-116180	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-rhcx-5729-88vg	vLLM
204	vLLM 服务端请求伪造漏洞	CNNVD-2026-66286226	CVE-2026-116176	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-vfp2-c8pq-v6h6	vLLM
205	vLLM 资源管理错误漏洞	CNNVD-2026-50282348	CVE-2026-116175	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-r45p-7qwx-qwjw	vLLM
206	vLLM 输入验证错误漏洞	CNNVD-2026-58181693	CVE-2026-116174	高危	https://github.com/vll	vLLM

					m-project/vllm/security/advisories/GHSA-w2v2-5662-8v5q	
207	vLLM 输入验证错误漏洞	CNNVD-2026-15747854	CVE-2026-116173	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-6pgw-f3pv-4h8q	vLLM
208	vLLM 输入验证错误漏洞	CNNVD-2026-56431799	CVE-2026-116172	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-rwfw-xvg3-3937	vLLM
209	vLLM 资源管理错误漏洞	CNNVD-2026-97789435	CVE-2026-114052	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-823j-m4cj-hmjf	vLLM
210	vLLM 资源管理错误漏洞	CNNVD-2026-54157834	CVE-2026-114055	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-gx7p-2j49-hfq4	vLLM
211	vLLM 权限许可和访问控制问题漏洞	CNNVD-2026-32618285	CVE-2026-114054	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-rh6f-3x46-j33q	vLLM
212	vLLM 异常处理	CNNVD-2026-	CVE-2026-	高危	https://git	vLLM

	不当漏洞	85025454	114051		hub.com/vllm-project/vllm/security/advisories/GHSA-4xqp-c3mv-qff7	
213	vLLM 输入验证错误漏洞	CNNVD-2026-85629691	CVE-2026-114050	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-p92p-rxj5-7p2x	vLLM
214	VTK 缓冲区错误漏洞	CNNVD-2026-24696684	CVE-2026-9536	高危	https://vtk.org/download/	VTK
215	VTK 缓冲区错误漏洞	CNNVD-2026-71934162	CVE-2026-9535	高危	https://vtk.org/download/	VTK
216	VTK 缓冲区错误漏洞	CNNVD-2026-24824390	CVE-2026-8824	高危	https://vtk.org/download/	VTK
217	VTK 缓冲区错误漏洞	CNNVD-2026-16999719	CVE-2026-8822	高危	https://vtk.org/download/	VTK
218	VTK 资源管理错误漏洞	CNNVD-2026-73166166	CVE-2026-42057	高危	https://vtk.org/	VTK
219	VTK 资源管理错误漏洞	CNNVD-2026-95256918	CVE-2026-41216	高危	https://vtk.org/download/	VTK
220	WordPress AI Engine 跨站脚本漏洞	CNNVD-2026-32412594	CVE-2026-96561	高危	https://wordpress.org/plugins/ai-engine/	WordPress
221	WordPress MxChat 跨站脚本漏洞	CNNVD-2026-25162924	CVE-2026-110662	高危	https://wordpress.org/plugins/mxchat-basic/	WordPress
222	Xorbits Inference 路径遍历漏洞	CNNVD-2026-23179514	CVE-2026-112051	高危	https://github.com/xorbitsai/inference/commit/beddc97ac211f8414597fe8479493be	Xorbits

					0603f7c84	
223	北京智谱华章 ZCode 安全漏洞	CNNVD-2026-23231856	CVE-2026-88755	高危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	北京智谱华章
224	ageerle RuoYi AI 授权问题漏洞	CNNVD-2026-35852916	CVE-2026-108112	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	ageerle
225	ageerle RuoYi AI 授权问题漏洞	CNNVD-2026-70822768	CVE-2026-108111	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	ageerle
226	Agent Zero 安全漏洞	CNNVD-2026-83133838	CVE-2026-51852	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Agent Zero
227	Agent Zero 安全漏洞	CNNVD-2026-58731819	CVE-2026-51851	中危	目前厂商暂未发布修复	Agent Zero

					措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
228	AgentScope-AI agentscope 安全漏洞	CNNVD-2026-89182085	CVE-2026-51922	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	AgentScope-AI
229	Agno 处理逻辑错误漏洞	CNNVD-2026-44095864	CVE-2026-108819	中危	https://github.com/ybyu-ieu/agno-security-advisories/blob/main/advisories/agno-agent-orchestration-missing-confirmation-gate-code-execution.md	Agno
230	Agno 授权问题漏洞	CNNVD-2026-71774149	CVE-2026-108818	中危	https://github.com/ybyu-ieu/agno-security-advisories/blob/main/advisories/agno-agentos-no-authentication-by-default.md	Agno

231	AI4Finance FinRobot 安全漏洞	CNNVD-2026-85882606	CVE-2026-51917	中危	https://github.com/AI4Finance-Foundation/FinRobot/releases	AI4Finance
232	AI4Finance FinRobot 安全漏洞	CNNVD-2026-23561654	CVE-2026-51918	中危	https://github.com/AI4Finance-Foundation/FinRobot/releases	AI4Finance
233	camel-ai camel 安全漏洞	CNNVD-2026-29949473	CVE-2026-51858	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	camel-ai
234	camel-ai camel 安全漏洞	CNNVD-2026-88187753	CVE-2026-51857	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	camel-ai
235	Carmine Paolino ruby_llm 安全漏洞	CNNVD-2026-93865858	CVE-2026-67987	中危	https://github.com/crmne/ruby_llm/commit/5e88411f171721b381853fa77d254e266dcf6ad8	Carmine Paolino
236	CASIA-LMC-Lab Fast Segment Anything 代码注入漏洞	CNNVD-2026-28958674	CVE-2026-111237	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此	CASIA-LMC-Lab

					软件的用户随时关注厂商主页或参考网址以获取解决办法。	
237	Chatchat-Space Langchain-Chatchat 安全漏洞	CNNVD-2026-10176631	CVE-2026-51883	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Chatchat-Space
238	Chatchat-Space Langchain-Chatchat 安全漏洞	CNNVD-2026-46275580	CVE-2026-51882	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Chatchat-Space
239	ChatGPTNextWeb NextChat 服务端请求伪造漏洞	CNNVD-2026-52671873	CVE-2026-105238	中危	https://github.com/ChatGPTNextWeb/NextChat/issues/6813	ChatGPTNextWeb
240	Cheshire Cat AI 跨站脚本漏洞	CNNVD-2026-61345444	CVE-2026-108725	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Cheshire Cat AI
241	Cohere Python SDK 路径遍历漏洞	CNNVD-2026-98821156	CVE-2026-108597	中危	目前厂商暂未发布修复措施解决此	Cohere

					安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
242	Data Intelligence Lab@HKU AnyTool 命令注入漏洞	CNNVD-2026-12895006	CVE-2026-102874	中危	https://github.com/HKUDS/AnyTool/issues/6	Data Intelligence Lab@HKU
243	Databricks Mosaic Research Composer 路径遍历漏洞	CNNVD-2026-27735644	CVE-2026-109153	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Databricks Mosaic Research
244	decolua 9Router 服务端请求伪造漏洞	CNNVD-2026-96646075	CVE-2026-103530	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	decolua
245	DeepSeek Harness 权限许可和访问控制问题漏洞	CNNVD-2026-90522926	CVE-2026-101102	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	DeepSeek
246	DeepSeek	CNNVD-2026-	CVE-2026-	中危	目前厂商暂	DeepSeek

	Harness 安全漏洞	93031746	95183		未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
247	Discourse 跨站脚本漏洞	CNNVD-2026-20704988	CVE-2017-20290	中危	https://github.com/discourse/discourse/commit/6e37f09b19,https://github.com/discourse/discourse/commit/a6f2533d38	Discourse
248	Drupal Artificial Intelligence 授权问题漏洞	CNNVD-2026-30584080	CVE-2026-84912	中危	https://www.drupal.org/sa-contrib-2026-120	Drupal
249	Dyad 跨站请求伪造漏洞	CNNVD-2026-94846082	CVE-2026-111988	中危	https://github.com/dyad-sh/dyad/security/advisories/GHSA-pqj5-w36j-2839	Dyad
250	EleutherAI Language Model Evaluation Harness 服务端请求伪造漏洞	CNNVD-2026-78646682	CVE-2026-17557	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	EleutherAI
251	eosphoros DB-GPT 安全漏洞	CNNVD-2026-69540207	CVE-2026-51869	中危	目前厂商暂未发布修复	eosphoros

					措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
252	eosphoros DB-GPT 安全漏洞	CNNVD-2026-79231977	CVE-2026-51862	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	eosphoros
253	eosphoros DB-GPT 安全漏洞	CNNVD-2026-21929498	CVE-2026-51863	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	eosphoros
254	Eric Buehler mistral.rs 路径遍历漏洞	CNNVD-2026-17351846	CVE-2026-108940	中危	https://github.com/EricLBuehler/mistral.rs/commit/8c8105671	Eric Buehler
255	Eric Buehler mistral.rs 服务端请求伪造漏洞	CNNVD-2026-16511669	CVE-2026-108939	中危	https://github.com/EricLBuehler/mistral.rs/commit/cfb8c6a0c42361dc4579a9110b54d339c255b9fd	Eric Buehler
256	Francois	CNNVD-2026-	CVE-2026-	中危	https://git	Francois

	Jacquet RosarioSIS 授权问题漏洞	91592883	116010		lab.com/francoisjacquet/rosariosis/-/releases/v12.9.1	Jacquet
257	ggml llama.cpp 异常处理不当漏洞	CNNVD-2026-86745397	CVE-2026-116467	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	ggml
258	Google OSV-SCALIBR 路径遍历漏洞	CNNVD-2026-69780164	CVE-2026-102252	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Google
259	Helicone 服务端请求伪造漏洞	CNNVD-2026-94070975	CVE-2026-108602	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Helicone
260	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-36261836	CVE-2026-104331	中危	https://www.ibm.com/support/pages/node/7293015	IBM
261	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-49373143	CVE-2026-104316	中危	https://www.ibm.com/support/pages	IBM

					/node/7293015	
262	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-14679227	CVE-2026-104315	中危	https://www.ibm.com/support/pages/node/7293015	IBM
263	IBM Langflow OSS 信任管理问题漏洞	CNNVD-2026-22853322	CVE-2026-104314	中危	https://www.ibm.com/support/pages/node/7293015	IBM
264	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-36581058	CVE-2026-104310	中危	https://www.ibm.com/support/pages/node/7293015	IBM
265	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-58733633	CVE-2026-104309	中危	https://www.ibm.com/support/pages/node/7293015	IBM
266	IBM Langflow OSS 命令注入漏洞	CNNVD-2026-28802756	CVE-2026-104308	中危	https://www.ibm.com/support/pages/node/7293015	IBM
267	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-56435802	CVE-2026-102590	中危	https://www.ibm.com/support/pages/node/7293015	IBM
268	IBM Langflow OSS 资源管理错误漏洞	CNNVD-2026-28843471	CVE-2026-90991	中危	https://www.ibm.com/support/pages/node/7293016	IBM
269	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-76421554	CVE-2026-77819	中危	https://www.ibm.com/support/pages/node/7293015	IBM
270	IBM Langflow OSS 信息泄露漏洞	CNNVD-2026-70319330	CVE-2026-77817	中危	https://www.ibm.com/support/pages/node/7293016	IBM

271	IBM Planning Analytics 跨站脚本漏洞	CNNVD-2026-86164009	CVE-2026-75063	中危	https://www.ibm.com/support/pages/node/7291604	IBM
272	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-92455743	CVE-2026-97671	中危	https://www.ibm.com/support/pages/node/7290694	IBM
273	IBM Planning Analytics 跨站脚本漏洞	CNNVD-2026-71144661	CVE-2026-18541	中危	https://www.ibm.com/support/pages/node/7291604	IBM
274	IBM Langflow OSS 资源管理错误漏洞	CNNVD-2026-91323919	CVE-2026-93679	中危	https://www.ibm.com/support/pages/node/7290694	IBM
275	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-83789079	CVE-2026-93448	中危	https://www.ibm.com/support/pages/node/7290694	IBM
276	IBM Langflow OSS 加密问题漏洞	CNNVD-2026-88506088	CVE-2026-110200	中危	https://www.ibm.com/support/pages/node/7293016	IBM
277	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-66582816	CVE-2026-110190	中危	https://www.ibm.com/support/pages/node/7293016	IBM
278	IBM Langflow OSS 信任管理问题漏洞	CNNVD-2026-27158397	CVE-2026-110192	中危	https://www.ibm.com/support/pages/node/7294467	IBM
279	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-57265692	CVE-2026-18894	中危	https://www.ibm.com/support/pages/node/7293016	IBM
280	iFLYTEK Astron Agent 输入验证	CNNVD-2026-67916230	CVE-2026-116339	中危	目前厂商暂未发布修复	iFLYTEK

	错误漏洞				措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
281	iMoon YOLOv13 输入验证错误漏洞	CNNVD-2026-53922260	CVE-2026-108945	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	iMoon
282	InfiniFlow RAGFlow 安全漏洞	CNNVD-2026-99401040	CVE-2026-51897	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	InfiniFlow
283	InfiniFlow RAGFlow 权限许可和访问控制问题漏洞	CNNVD-2026-70677171	CVE-2026-51895	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	InfiniFlow
284	Jovan Marinovic Network-AI 输入验证错误漏洞	CNNVD-2026-65549131	CVE-2026-109330	中危	https://github.com/Jovancoding/Network-AI/security	Jovan Marinovic

					/advisories/GHSA-hr6v-mfxm-4438	
285	Khronos Group NNEF-Tools 路径遍历漏洞	CNNVD-2026-60188708	CVE-2026-110657	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Khronos Group
286	kilocode 安全漏洞	CNNVD-2026-30789145	CVE-2026-79403	中危	https://github.com/Kilo-Org/kilocode/commit/51e45d7fb7	Kilo Code
287	KNIME Business Hub 权限许可和访问控制问题漏洞	CNNVD-2026-42447679	CVE-2026-115517	中危	https://www.knime.com/security/advisories	KNIME
288	KNIME Business Hub 授权问题漏洞	CNNVD-2026-11013260	CVE-2026-115502	中危	https://www.knime.com/security/advisories	KNIME
289	KNIME Business Hub 信息泄露漏洞	CNNVD-2026-77918018	CVE-2026-115496	中危	https://www.knime.com/security/advisories	KNIME
290	KNIME Business Hub 跨站请求伪造漏洞	CNNVD-2026-92566714	CVE-2026-115494	中危	https://www.knime.com/security/advisories	KNIME
291	KNIME Business Hub 资源管理错误漏洞	CNNVD-2026-38091888	CVE-2026-115454	中危	https://www.knime.com/security/advisories	KNIME
292	KNIME Analytics Platform 日志信息泄露漏洞	CNNVD-2026-69976944	CVE-2026-115657	中危	https://www.knime.com/security/advisories	KNIME
293	kvcache-ai Mooncake 授权问题漏洞	CNNVD-2026-38774873	CVE-2026-96762	中危	https://github.com/kvcache-	kvcache-ai

					ai/Mooncake/releases	
294	LangChain Chatchat 安全漏洞	CNNVD-2026-88375432	CVE-2026-51884	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	LangChain
295	LangChain LangGraph 日志信息泄露漏洞	CNNVD-2026-37150540	CVE-2026-115885	中危	https://github.com/langchain-ai/langgraph/security/advisories/GHSA-8prr-f582-jqq3	LangChain
296	LangChain LangGraph 输入验证错误漏洞	CNNVD-2026-81004097	CVE-2026-115883	中危	https://github.com/langchain-ai/langgraph/security/advisories/GHSA-6hmw-9432-67qq	LangChain
297	LMCache 授权问题漏洞	CNNVD-2026-49547978	CVE-2026-107207	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	LMCache
298	Massimiliano Pippi banks 输入验证错误漏洞	CNNVD-2026-48259502	CVE-2026-107717	中危	https://github.com/masci/banks/releases/tag/v2.5.0	Massimiliano Pippi
299	Mem0 信息泄露漏洞	CNNVD-2026-46728544	CVE-2026-116575	中危	https://github.com/mem	Mem0

					0ai/mem0/security/advisories/GHSA-5324-3w58-qpp2	
300	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-93238935	CVE-2026-62179	中危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-mxmx-rh57-jx58	Mervin Praison
301	MLflow 信息泄露漏洞	CNNVD-2026-92922287	CVE-2026-116691	中危	https://github.com/mlflow/mlflow/security/advisories/GHSA-j7qq-vr8c-xvw3	MLflow
302	MLflow 代码注入漏洞	CNNVD-2026-77014698	CVE-2026-115886	中危	https://github.com/mlflow/mlflow/releases/tag/v3.17.0	MLflow
303	NetEase Youdao LobsterAI 输入验证错误漏洞	CNNVD-2026-41585372	CVE-2026-108156	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	NetEase Youdao
304	NetEase Youdao LobsterAI 加密问题漏洞	CNNVD-2026-48059593	CVE-2026-112014	中危	https://github.com/netease-youdao/LobsterAI/commit/1eb28c40d7e42d6cbade07874e6f6c068b6a9a64,https://github.com/nete	NetEase Youdao

					ase-youdao/LobsterAI/releases/tag/2026.10.16	
305	NextChat 跨站脚本漏洞	CNNVD-2026-17738809	CVE-2026-118132	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	NextChat
306	Nous Research Hermes Agent 授权问题漏洞	CNNVD-2026-75503096	CVE-2026-114463	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Nous Research
307	ntop nDPI 缓冲区错误漏洞	CNNVD-2026-37378463	CVE-2026-116744	中危	https://github.com/ntop/nDPI/commit/ca9d819151606377ac53305583fe819748c69be2	ntop
308	NVIDIA TensorRT 缓冲区错误漏洞	CNNVD-2026-88177652	CVE-2026-65122	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	NVIDIA
309	NVIDIA virtual gpu manager 缓	CNNVD-2026-84633363	CVE-2026-47544	中危	https://www.nvidia.com	NVIDIA

	冲区错误漏洞				/en-us/security/	
310	NVIDIA virtual gpu manager 数字错误漏洞	CNNVD-2026-72645203	CVE-2026-47539	中危	https://www.nvidia.com/en-us/security/	NVIDIA
311	Obot AI Obot 授权问题漏洞	CNNVD-2026-17660800	CVE-2026-105139	中危	https://github.com/obot-platform/obot/security/advisories/GHSA-xhpw-65qw-wj6m	Obot AI
312	Ollama 服务端请求伪造漏洞	CNNVD-2026-46712083	CVE-2026-108836	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Ollama
313	OpenBMB XAgent 安全漏洞	CNNVD-2026-45233540	CVE-2026-51912	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	OpenBMB
314	OpenClaw 授权问题漏洞	CNNVD-2026-15274086	CVE-2026-102807	中危	https://docs.openclaw.ai/releases/2026.9.4	OpenClaw
315	OpenClaw 授权问题漏洞	CNNVD-2026-79797221	CVE-2026-102806	中危	https://docs.openclaw.ai/releases/2026.9.5	OpenClaw
316	OpenStack	CNNVD-2026-	CVE-2026-	中危	https://sec	OpenStack

	Mistral 授权问题漏洞	75495777	93861		urity.openstack.org/ossa/OSSA-2026-044.html	
317	PaddlePaddle PaddleX 输入验证错误漏洞	CNNVD-2026-11821659	CVE-2026-108961	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	PaddlePaddle
318	philz1337x Clarity AI 跨站脚本漏洞	CNNVD-2026-64116075	CVE-2026-108942	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	philz1337x
319	Plastic Labs honcho 授权问题漏洞	CNNVD-2026-90859493	CVE-2026-108711	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Plastic Labs
320	pulseaiclub phi 后置链接漏洞	CNNVD-2026-12698940	CVE-2026-108599	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获	pulseaiclub

					取解决办法。	
321	pulseaiclub phi 授权问题漏洞	CNNVD-2026-78340562	CVE-2026-108595	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	pulseaiclub
322	pydantic-ai 资源管理错误漏洞	CNNVD-2026-28273817	CVE-2026-114386	中危	https://github.com/pydantic/pydantic-ai/commit/eb27b2b89fe76ae23ee9b6fc9eb4b227a4967949	Pydantic
323	Pydantic pydantic-ai 资源管理错误漏洞	CNNVD-2026-16425263	CVE-2026-107294	中危	https://github.com/pydantic/pydantic-ai/releases	Pydantic
324	Pydantic pydantic-ai 输入验证错误漏洞	CNNVD-2026-15651108	CVE-2026-107292	中危	https://github.com/pydantic/pydantic-ai/releases	Pydantic
325	Pydantic pydantic-ai 资源管理错误漏洞	CNNVD-2026-34917759	CVE-2026-107290	中危	https://github.com/pydantic/pydantic-ai/releases	Pydantic
326	Pydantic pydantic-ai 输入验证错误漏洞	CNNVD-2026-12189793	CVE-2026-107289	中危	https://github.com/pydantic/pydantic-ai/releases	Pydantic
327	Pydantic pydantic-ai 资源管理错误漏洞	CNNVD-2026-84363372	CVE-2026-107287	中危	https://github.com/pydantic/pydantic-ai/releases	Pydantic

328	REBUILD 授权问题漏洞	CNNVD-2026-62979350	CVE-2026-102249	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	REBUILD
329	REBUILD 授权问题漏洞	CNNVD-2026-29291189	CVE-2026-102248	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	REBUILD
330	Refly AI Refly 信任管理问题漏洞	CNNVD-2026-70976250	CVE-2026-101052	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Refly AI
331	Reworkd AgentGPT 安全漏洞	CNNVD-2026-13565322	CVE-2026-51867	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Reworkd
332	Rohan Verma SurfSense 授权问题漏洞	CNNVD-2026-23872410	CVE-2026-102245	中危	目前厂商暂未发布修复措施解决此	Rohan Verma

					安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
333	ServiceNow AI Platform 权限许可和访问控制问题漏洞	CNNVD-2026-77450355	CVE-2026-6877	中危	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3228994	ServiceNow
334	sgl-project SGLang 授权问题漏洞	CNNVD-2026-99262131	CVE-2026-112268	中危	https://github.com/sgl-project/sglang/releases	sgl-project
335	sgl-project SGLang 服务端请求伪造漏洞	CNNVD-2026-12588639	CVE-2026-112267	中危	https://github.com/sgl-project/sglang/releases	sgl-project
336	sgl-project SGLang 资源管理错误漏洞	CNNVD-2026-72628116	CVE-2026-112083	中危	https://github.com/sgl-project/sglang/releases	sgl-project
337	sgl-project SGLang 输入验证错误漏洞	CNNVD-2026-87427652	CVE-2026-111392	中危	https://github.com/sgl-project/sglang/releases	sgl-project
338	smub All in One SEO 代码注入漏洞	CNNVD-2026-27023692	CVE-2026-100152	中危	https://wordpress.org/plugins/all-in-one-seo-pack/	smub
339	smub All in One SEO 跨站脚	CNNVD-2026-73705716	CVE-2026-85492	中危	https://wordpress.org/	smub

	本漏洞				plugins/all-in-one-seo-pack/	
340	stition Devika 安全漏洞	CNNVD-2026-94039658	CVE-2026-51875	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	stition
341	stition Devika 安全漏洞	CNNVD-2026-10857284	CVE-2026-51874	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	stition
342	Strands Agents Tools 提示词注入漏洞	CNNVD-2026-62132273	CVE-2026-115415	中危	https://github.com/strands-agents/tools/security/advisories/GHSA-qjx4-hg6g-2f34	strands-agents
343	SuperAGI 安全漏洞	CNNVD-2026-24401143	CVE-2026-51903	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	SuperAGI
344	SuperAGI 安全漏洞	CNNVD-2026-42109036	CVE-2026-51905	中危	目前厂商暂未发布修复措施解决此	SuperAGI

					安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
345	SuperAGI 安全漏洞	CNNVD-2026-34240680	CVE-2026-51902	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	SuperAGI
346	TaskingAI 服务端请求伪造漏洞	CNNVD-2026-19674001	CVE-2026-111321	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	TaskingAI
347	Tencent WeKnora 服务端请求伪造漏洞	CNNVD-2026-46275689	CVE-2026-118376	中危	https://github.com/Tencent/WeKnora/commit/d7ccd5ba517cc3968e6d5000a2ab0f4b51ef1dda,https://github.com/Tencent/WeKnora/commit/ff818b681f10bc29edbc48fe35f00009dc276bfa,https://github.com/Te	Tencent

					ncent/WeKnora/releases/tag/v0.8.2	
348	Topoteretes Cognee 信任管理问题漏洞	CNNVD-2026-74754542	CVE-2026-105141	中危	https://github.com/topoteretes/cognee	Topoteretes
349	Turboderp exllamav3 缓冲区错误漏洞	CNNVD-2026-61370469	CVE-2026-84286	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	Turboderp
350	UnicomAI Wanwu 授权问题漏洞	CNNVD-2026-23233896	CVE-2026-108854	中危	https://github.com/UnicomAI/wanwu/releases/tag/v0.6.3	UnicomAI
351	UnicomAI Wanwu 授权问题漏洞	CNNVD-2026-57183126	CVE-2026-108855	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	UnicomAI
352	ValueCell.ai ValueCell 服务端请求伪造漏洞	CNNVD-2026-52751628	CVE-2026-111320	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	ValueCell.ai
353	Vanna AI Vanna 安全漏洞	CNNVD-2026-96130034	CVE-2026-51911	中危	目前厂商暂未发布修复	Vanna AI

					措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	
354	vLLM 资源管理错误漏洞	CNNVD-2026-67886086	CVE-2026-115918	中危	https://github.com/vllm-project/vllm/security/advisories/GHSA-x567-49g5-p4cf	vLLM
355	vLLM 输入验证错误漏洞	CNNVD-2026-88528670	CVE-2026-115916	中危	https://github.com/vllm-project/vllm/security/advisories/GHSA-q97c-p368-75c4	vLLM
356	vLLM 资源管理错误漏洞	CNNVD-2026-32518428	CVE-2026-115913	中危	https://github.com/vllm-project/vllm/security/advisories/GHSA-8397-8qf6-f2gm	vLLM
357	vLLM 资源管理错误漏洞	CNNVD-2026-58895468	CVE-2026-115911	中危	https://github.com/vllm-project/vllm/security/advisories/GHSA-542m-9234-8gvf	vLLM
358	vLLM 处理逻辑错误漏洞	CNNVD-2026-12778589	CVE-2026-114049	中危	https://github.com/vllm-project/vllm/security/advisories/	vLLM

					GHSA-6cxc-2vcg-w5qc	
359	vLLM 异常处理不当漏洞	CNNVD-2026-58378914	CVE-2026-115914	中危	https://github.com/vllm-project/vllm/security/advisories/GHSA-gq5q-89c7-vhvx	vLLM
360	WordPress AI Engine 路径遍历漏洞	CNNVD-2026-57780821	CVE-2026-107745	中危	https://wordpress.org/plugins/ai-engine/	WordPress
361	WordPress AI Engine 授权问题漏洞	CNNVD-2026-92254308	CVE-2026-110888	中危	https://wordpress.org/plugins/ai-engine/	WordPress
362	YuePeng ERUPT SQL 注入漏洞	CNNVD-2026-79084639	CVE-2026-111390	中危	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法。	YuePeng
363	Zylon PrivateGPT 服务端请求伪造漏洞	CNNVD-2026-47114850	CVE-2026-116000	中危	https://github.com/zylon-ai/private-gpt/issues/2269,https://github.com/zylon-ai/private-gpt/security/advisories/GHSA-8294-hj7x-42g2	Zylon

（三）重要人工智能漏洞实例

近期重要漏洞实例如表 2 所示。

表 2 本期重要漏洞实例

序号	漏洞编号	危害等级
1	CNNVD-2026-41538350	超危
2	CNNVD-2026-55699613	高危
3	CNNVD-2026-64890438	高危

1. DeepSeek 信息泄露漏洞（CNNVD-2026-41538350）

DeepSeek 是中国 DeepSeek 公司的一个大语言模型。

DeepSeek V4 存在信息泄露漏洞，该漏洞源于访问控制不当，攻击者利用该漏洞可以获取敏感信息。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://www.deepseek.com/

2. sgl-project SGLang 资源管理错误漏洞（CNNVD-2026-55699613）

sgl-project SGLang 是 sgl-project 组织开源的一个用于加速大模型推理的编程语言与运行时系统。

sgl-project SGLang 0.5.22 及之前版本存在资源管理错误漏洞，该漏洞源于内存分配不当，攻击者利用该漏洞可以耗尽内存导致系统终止运行。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://github.com/sgl-project/sglang/releases

3. Mervin Praison PraisonAI 输入验证错误漏洞（CNNVD-2026-64890438）

Mervin Praison PraisonAI 是 Mervin Praison 个人开发者开源的一个低代码多智能体协作框架。

Mervin Praison PraisonAI 1.6.62 之前版本存在安全漏洞，该漏洞源于未对主机、端口或解析地址进行验证，攻击者利用该漏洞可以获取敏感信息。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-4pcv-mg8v-vrgf