人工智能重要漏洞通报

（2026 年第十四期）

根据国家人工智能安全漏洞库（AIVD）统计，近期（2026 年 9 月 3 日至 2026 年 9 月 28 日）共采集重要人工智能漏洞 392 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 Google（Gemini）、FlowiseAI、OpenClaw 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 64 个，高危漏洞 193 个，中危漏洞 135 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 392 个。

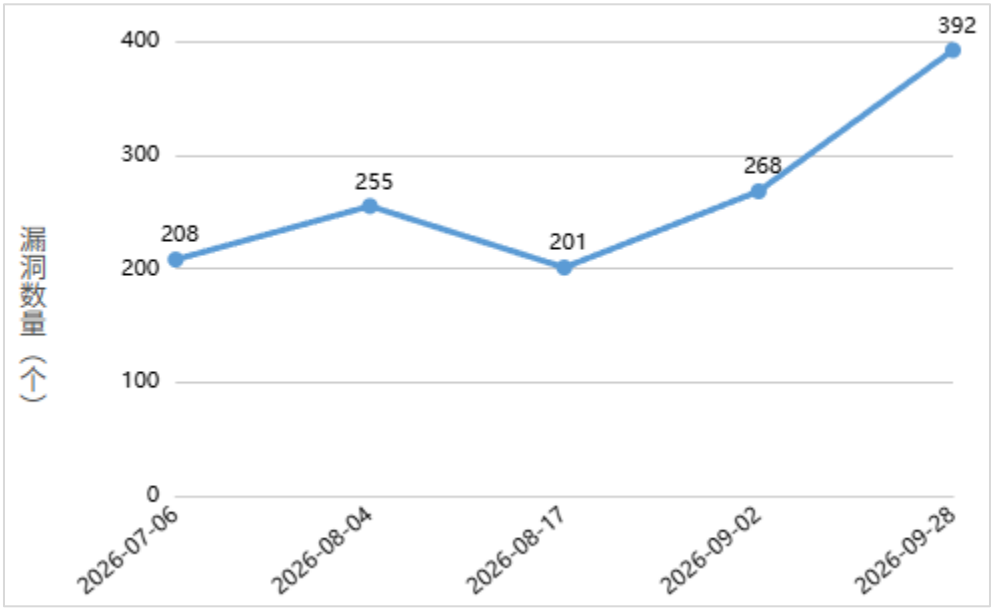


图 1 近期漏洞新增数量统计图

（二）人工智能漏洞具体情况

近期共采集重要人工智能漏洞 392 个，包括 Google（Gemini）、FlowiseAI、OpenClaw 等多个厂商（项目）的漏洞。其中超危漏洞 64 个，高危漏洞 193 个，中危漏洞 135 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	Aim 授权问题漏洞	CNNVD-2026-99919620	CVE-2026-85663	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。	Aim
2	Angel 反序列化注入漏洞	CNNVD-2026-53262818	CVE-2026-92785	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。	Angel
3	Apache Software Foundation Apache OpenNLP 输入验证错误漏洞	CNNVD-202605-461	CVE-2026-40682	超危	https://lists.apache.org/thread/r6jpt0qr9nj67gqhppqg7jxf8vsbo0w6	Apache Software Foundation
4	Avaiga Taipy 输入验证错误漏洞	CNNVD-2026-48991633	CVE-2026-85183	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	Avaiga

					商主页或参考网址以获取解决办法。	
5	Cua AI Cua 授权问题漏洞	CNNVD-2026-13234478	CVE-2026-86121	超危	https://github.com/trycua/cua/commit/59cf25c0ec54	Cua AI
6	Data Intelligence Lab@HKU AutoAgent 授权问题漏洞	CNNVD-2026-82938613	CVE-2026-86124	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。	Data Intelligence Lab@HKU
7	Data Intelligence Lab@HKU nanobot 服务端请求伪造漏洞	CNNVD-2026-60971262	CVE-2026-92576	超危	https://github.com/HKUDS/nanobot/security/advisories/GHSA-vc5v-6vwm-wf9m	Data Intelligence Lab@HKU
8	Data Intelligence Lab@HKU LightRAG 授权问题漏洞	CNNVD-2026-28298531	CVE-2026-85734	超危	https://github.com/HKUDS/LightRAG/security/advisories/GHSA-frch-4w6v-q5xx	Data Intelligence Lab@HKU
9	Feast 信任管理问题漏洞	CNNVD-2026-75352983	CVE-2026-92787	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。	Feast
10	FlowiseAI Flowise 输入验	CNNVD-2026-83660513	CVE-2026-91932	超危	https://github.com/Flo	FlowiseAI

	证错误漏洞				wiseAI/Flowise/security/advisories/GHSA-x7x8-95gh-42xm	
11	FlowiseAI Flowise 命令注入漏洞	CNNVD-2026-51457299	CVE-2026-91931	超危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-vcwp-f9rq-3887	FlowiseAI
12	FlowiseAI Flowise 代码注入漏洞	CNNVD-2026-91641538	CVE-2026-52098	超危	https://github.com/FlowiseAI/Flowise/releases	FlowiseAI
13	FlowiseAI Flowise 授权问题漏洞	CNNVD-2026-35070800	CVE-2026-100607	超危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-cffm-583c-vffr	FlowiseAI
14	FlowiseAI Flowise 授权问题漏洞	CNNVD-2026-72643920	CVE-2026-100606	超危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-vf3j-89vf-r697	FlowiseAI
15	Google Android XR 安全漏洞	CNNVD-2026-33893482	CVE-2026-28659	超危	https://source.android.com/docs/security/bulletin/xr/2026/2026-09-01	Google
16	Google Gemini CLI 输入验证错误漏洞	CNNVD-2026-43908055	CVE-2026-13745	超危	https://github.com/google-github-actions/run-gemini-	Google

					cli/security/advisories/GHSA-wpqr-6v78-jr5g	
17	Haris Excel MCP Server 路径遍历漏洞	CNNVD-2026-51701203	CVE-2026-85661	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。	Haris
18	huggingface huggingface/transformers 软件供应链问题漏洞	CNNVD-202606-699	CVE-2026-5241	超危	https://github.com/huggingface/transformers/commit/676559d5022b74aaa0cee1cee0842b7f27c5320e	huggingface
19	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-21113746	CVE-2026-81204	超危	https://www.ibm.com/support/pages/node/7286666	IBM
20	IBM Langflow OSS 命令注入漏洞	CNNVD-2026-30234359	CVE-2026-79724	超危	https://www.ibm.com/support/pages/node/7286666	IBM
21	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-21878827	CVE-2026-12944	超危	https://www.ibm.com/support/pages/node/7278919	IBM
22	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-72156633	CVE-2026-85025	超危	https://www.ibm.com/support/pages/node/7286666	IBM
23	InternLM LMDeploy 反序	CNNVD-2026-24292135	CVE-2025-66455	超危	https://github.com/Int	InternLM

	列化注入漏洞				ernLM/lmdeploy/security/advisories/GHSA-2vh9-42vm-xmv2	
24	InternLM LMDeploy 反序列化注入漏洞	CNNVD-2026-63684530	CVE-2025-59953	超危	https://github.com/InternLM/lmdeploy/security/advisories/GHSA-5h8j-6crg-7rmw	InternLM
25	LangBot HQ LangBot 加密问题漏洞	CNNVD-2026-91948344	CVE-2026-90562	超危	https://github.com/langbot-app/LangBot/commit/267232c24f93c515d6fd3f7f81c0676066ab1ab8	LangBot HQ
26	lavague 代码注入漏洞	CNNVD-2026-22442895	CVE-2026-85694	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。	lavague
27	LMSYS FastChat 授权问题漏洞	CNNVD-2026-29756969	CVE-2026-85695	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。	LMSYS
28	MAIC OpenMAIC 授权问题漏洞	CNNVD-2026-31588591	CVE-2026-86259	超危	https://github.com/THU	MAIC

					-MAIC/OpenMAIC/security/advisories/GHSA-9m7h-vh2h-rc3w	
29	Maxim AI Bifrost AI Gateway 权限许可和访问控制问题漏洞	CNNVD-2026-31744155	CVE-2026-90898	超危	https://github.com/maximhq/bifrost/commit/12e170352bd25eab1ae9ba16611f1797d1fd8fdc	Maxim AI
30	Mervin Praison PraisonAI 配置错误漏洞	CNNVD-2026-77933041	CVE-2026-57147	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-cwj8-7gp2-ggcw	Mervin Praison
31	Mervin Praison PraisonAI 配置错误漏洞	CNNVD-2026-69678283	CVE-2026-57148	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-f38v-77qj-h4jq	Mervin Praison
32	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-22320056	CVE-2026-57140	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-9752-mhqh-h34f	Mervin Praison
33	Mervin Praison PraisonAI 代码注入漏洞	CNNVD-2026-21341990	CVE-2026-57141	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-p69m-4f92-2v84	Mervin Praison
34	Mervin Praison	CNNVD-2026-	CVE-2026-	超危	https://git	Mervin

	PraisonAI 配置错误漏洞	23233133	57139		hub.com/MervinPraison/PraisonAI/security/advisories/GHSA-j4f3-55x4-r6q2	Praison
35	Mervin Praison PraisonAI 输入验证错误漏洞	CNNVD-2026-84846683	CVE-2026-57138	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-vmmj-pfw7-fjwp	Mervin Praison
36	Mervin Praison PraisonAI 路径遍历漏洞	CNNVD-2026-67842869	CVE-2026-57145	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-29w3-p9w9-wc47	Mervin Praison
37	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-72136470	CVE-2026-57131	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-fq2m-6wqh-x44g	Mervin Praison
38	Mervin Praison PraisonAI 配置错误漏洞	CNNVD-2026-92105860	CVE-2026-57123	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-x227-pf99-vffg	Mervin Praison
39	Mervin Praison PraisonAI 配置错误漏洞	CNNVD-2026-68037661	CVE-2026-57127	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-j4hj-7hfh-g2f4	Mervin Praison

40	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-18260799	CVE-2026-57125	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-4869-x4pr-q22x	Mervin Praison
41	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-52659372	CVE-2026-57124	超危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-p75f-6fp4-p57w	Mervin Praison
42	Microsoft Fabric 授权问题漏洞	CNNVD-2026-21949694	CVE-2026-69843	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69843	Microsoft
43	Microsoft Entra 授权问题漏洞	CNNVD-2026-87700721	CVE-2026-83941	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83941	Microsoft
44	Microsoft Azure AI Foundry 授权问题漏洞	CNNVD-2026-23502672	CVE-2026-85889	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85889	Microsoft
45	Microsoft Copilot Studio 加密问题漏洞	CNNVD-2026-61670837	CVE-2026-80098	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-	Microsoft

					80098	
46	Microsoft Azure AI Language Authoring 授权问题漏洞	CNNVD-2026-54571760	CVE-2026-70352	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70352	Microsoft
47	Microsoft Entra 授权问题漏洞	CNNVD-2026-57691503	CVE-2026-62916	超危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62916	Microsoft
48	Mistral AI Mistral Vibe 权限许可和访问控制问题漏洞	CNNVD-2026-69064954	CVE-2026-87988	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。	Mistral AI
49	Mistral AI Mistral Vibe 输入验证错误漏洞	CNNVD-2026-59497904	CVE-2026-87986	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。	Mistral AI
50	Mistral AI Mistral Vibe 配置错误漏洞	CNNVD-2026-60411136	CVE-2026-87987	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	Mistral AI

					考网址以获取解决办法。	
51	Mistral AI Mistral Vibe 输入验证错误漏洞	CNNVD-2026-35824091	CVE-2026-87985	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。	Mistral AI
52	Mistral AI Mistral Vibe 路径遍历漏洞	CNNVD-2026-50658462	CVE-2026-87983	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。	Mistral AI
53	Mistral AI Mistral Vibe 路径遍历漏洞	CNNVD-2026-64849609	CVE-2026-87984	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。	Mistral AI
54	ModelTC LightLLM 反序列化注入漏洞	CNNVD-2026-22652446	CVE-2026-90919	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。	ModelTC

55	ModelTC LightLLM 授权问题漏洞	CNNVD-2026-79729683	CVE-2026-93839	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。	ModelTC
56	ModelTC LightLLM 反序列化注入漏洞	CNNVD-2026-23486796	CVE-2026-96560	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。	ModelTC
57	OpenC3 COSMOS 代码注入漏洞	CNNVD-2026-13427241	CVE-2026-77602	超危	https://github.com/OpenC3/cosmos/security/advisories/GHSA-jjq7-m736-w977	OpenC3
58	OpenClaw 加密问题漏洞	CNNVD-2026-34619595	CVE-2026-100551	超危	https://github.com/openclaw/openclaw/security/advisories/GHSA-jjpc-p3xf-8g7p	OpenClaw
59	OpenTalker SadTalker 命令注入漏洞	CNNVD-2026-42691494	CVE-2026-85696	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	OpenTalker

					法。	
60	SciPhi-AI R2R SQL 注入漏洞	CNNVD-2026-71781258	CVE-2026-82526	超危	https://github.com/SciPhi-AI/R2R/issues/2309	SciPhi-AI
61	sgl-project sglang 反序列化注入漏洞	CNNVD-2026-64416107	CVE-2026-93088	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
62	Ultraviolet Cocos AI 输入验证错误漏洞	CNNVD-2026-63250110	CVE-2026-92701	超危	https://github.com/ultravioletrs/cocos/security/advisories/GHSA-4px3-wj2x-xx47	Ultraviolet
63	Ultraviolet Cocos AI 输入验证错误漏洞	CNNVD-2026-12631299	CVE-2026-92702	超危	https://github.com/ultravioletrs/cocos/security/advisories/GHSA-4r6g-mp48-j2rw	Ultraviolet
64	WordPress Everest Forms 反序列化注入漏洞	CNNVD-2026-41040160	CVE-2026-62103	超危	https://wordpress.org/plugins/everest-forms/	WordPress
65	AgentScope-AI AgentScope 路径遍历漏洞	CNNVD-2026-73575288	CVE-2026-85685	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	AgentScope-AI

					法。	
66	Aider AI aider 代码注入漏洞	CNNVD-2026-36734032	CVE-2026-85674	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
67	Ray 路径遍历漏洞	CNNVD-202603-3072	CVE-2026-32981	高危	https://github.com/ray-project/ray/releases	anyscale
68	Axolotl AI Axolotl 软件供应链问题漏洞	CNNVD-2026-48180207	CVE-2026-86169	高危	https://github.com/axolotl-ai-cloud/axolotl/releases/tag/v0.19.0	Axolotl AI
69	camel-ai OWL 服务端请求伪造漏洞	CNNVD-2026-36400001	CVE-2026-85675	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。	camel-ai
70	Cheshire Cat AI 授权问题漏洞	CNNVD-2026-62313863	CVE-2026-85093	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。	Cheshire Cat AI
71	Comfy Org	CNNVD-2026-	CVE-2026-	高危	目前厂商暂	Comfy Org

	ComfyUI 路径遍历漏洞	55850103	92816		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。	
72	coze-dev coze-studio 服务端请求伪造漏洞	CNNVD-2026-80832026	CVE-2026-92795	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。	coze-dev
73	coze-dev coze-studio 授权问题漏洞	CNNVD-2026-73421570	CVE-2026-92788	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。	coze-dev
74	CrewAI 权限许可和访问控制问题漏洞	CNNVD-2026-31645368	CVE-2026-37008	高危	https://github.com/crewAIInc/crewAI/commit/fb2323b3deb3ec62b3965526857e77a2264e4cd0	CrewAI
75	Data Intelligence Lab@HKU LightRAG 服务端请求伪造漏洞	CNNVD-2026-58658378	CVE-2026-85740	高危	https://github.com/HKUDS/LightRAG/security/advisories/GHSA-vv3m-f8x4-7377	Data Intelligence Lab@HKU

76	Datageartech DataGear 服务端请求伪造漏洞	CNNVD-2026-42021923	CVE-2026-92566	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。	Datageartech
77	Datalab Surya 输入验证错误漏洞	CNNVD-2026-23177237	CVE-2026-85687	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。	Datalab
78	decolua 9Router 输入验证错误漏洞	CNNVD-2026-30454288	CVE-2026-56681	高危	https://github.com/decolua/9router/security/advisories/GHSA-5mj8-gf6m-fhw8	decolua
79	DeepJavaLibrary Deep Java Library 数字错误漏洞	CNNVD-2026-27170848	CVE-2026-85228	高危	https://aws.amazon.com/security/security-bulletins/2026-106-aws/	DeepJavaLibrary
80	Discourse 跨站脚本漏洞	CNNVD-2026-53600761	CVE-2026-91122	高危	https://github.com/discourse/discourse/security/advisories/GHSA-8m44-f6g9-7cg7	Discourse
81	Discourse 路径遍历漏洞	CNNVD-2026-76314957	CVE-2026-91123	高危	https://github.com/discourse/disc	Discourse

					ourse/security/advisories/GHSA-6pwj-wgg8-4rjc	
82	eat-pray-ai yutu 输入验证错误漏洞	CNNVD-2026-81229982	CVE-2026-50158	高危	https://github.com/eat-pray-ai/yutu	eat-pray-ai
83	espnet 反序列化注入漏洞	CNNVD-2026-90093114	CVE-2026-90777	高危	https://github.com/espnet/espnet/security/advisories/GHSA-64f6-3gqc-r926	espnet
84	FaceFusion 路径遍历漏洞	CNNVD-2026-24761258	CVE-2026-84702	高危	https://github.com/facefusion/facefusion/releases/tag/3.7.0	FaceFusion
85	Feast 授权问题漏洞	CNNVD-2026-57091523	CVE-2026-55563	高危	https://github.com/feast-dev/feast/security/advisories/GHSA-2j2x-r73g-hrr5	Feast
86	FlowiseAI Flowise 服务端请求伪造漏洞	CNNVD-2026-19925514	CVE-2026-91938	高危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-9cvr-5wv9-2gxr	FlowiseAI
87	FlowiseAI Flowise 输入验证错误漏洞	CNNVD-2026-39717472	CVE-2026-91937	高危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-wpvf-4vfx-rgxm	FlowiseAI
88	FlowiseAI	CNNVD-2026-	CVE-2026-	高危	https://git	FlowiseAI

	Flowise 命令注入漏洞	26148278	91936		hub.com/FlowiseAI/Flowise/security/advisories/GHSA-jrcq-qjw5-xx5q	
89	FlowiseAI Flowise 服务端请求伪造漏洞	CNNVD-2026-71531247	CVE-2026-91935	高危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-hx55-h48h-7rw9	FlowiseAI
90	FlowiseAI Flowise 路径遍历漏洞	CNNVD-2026-14116056	CVE-2026-91934	高危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-pwfj-wh95-7mwp	FlowiseAI
91	FlowiseAI Flowise 授权问题漏洞	CNNVD-2026-98819826	CVE-2026-91933	高危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-gggp-6qmf-xwwc	FlowiseAI
92	FlowiseAI Flowise 权限许可和访问控制问题漏洞	CNNVD-2026-68446688	CVE-2026-91930	高危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-pprx-4prj-35mj	FlowiseAI
93	FlowiseAI Flowise 授权问题漏洞	CNNVD-2026-84589767	CVE-2026-91929	高危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-7x8x-vv46-4579	FlowiseAI

94	FlowiseAI Flowise 授权问题漏洞	CNNVD-2026-28132946	CVE-2026-100609	高危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-27w2-26m5-x82c	FlowiseAI
95	FlowiseAI Flowise 授权问题漏洞	CNNVD-2026-91088460	CVE-2026-100610	高危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-jvx3-mjpw-r4gh	FlowiseAI
96	FlowiseAI Flowise 授权问题漏洞	CNNVD-2026-71572176	CVE-2026-100608	高危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-rpcc-gw54-mfgx	FlowiseAI
97	FlowiseAI Flowise 授权问题漏洞	CNNVD-2026-47293146	CVE-2026-100605	高危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-ppmg-4cx6-95hh	FlowiseAI
98	ggml llama.cpp 安全漏洞	CNNVD-2026-86476237	CVE-2026-52132	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
99	Google Gemini Enterprise Agent Platform App Builder 服	CNNVD-2026-61244283	CVE-2026-19486	高危	https://docs.cloud.google.com/gemini-	Google

	务端请求伪造漏洞				enterprise-agent-platform/release-notes#July_20_2026	
100	Google Gemini Enterprise Agent Platform SDK for Python 加密问题漏洞	CNNVD-2026-20982479	CVE-2026-19407	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。	Google
101	headroomlabs-ai headroom 输入验证错误漏洞	CNNVD-2026-34879259	CVE-2026-71416	高危	https://github.com/headroomlabs-ai/headroom/security/advisories/GHSA-h46j-26q3-rggf	headroomlabs-ai
102	Helicone 授权问题漏洞	CNNVD-2026-41416589	CVE-2026-85178	高危	https://github.com/Helicone/helicone/commit/ca34549ea56f7ed587843f82d9cc19baa1f36ba4	Helicone
103	Hugging Face Tokenizers 缓冲区错误漏洞	CNNVD-2026-36655309	CVE-2026-85670	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
104	HumanSignal Label Studio 授权问题漏洞	CNNVD-2026-40506591	CVE-2026-85211	高危	目前厂商暂未发布修复措施解决此	HumanSignal

					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。	
105	HumanSignal Label Studio 服务端请求伪造漏洞	CNNVD-2026-68034646	CVE-2026-85179	高危	https://github.com/HumanSignal/label-studio/commit/2c1c1d6472153032af8ed399168f814bea854e3e	HumanSignal
106	IBM Langflow OSS 会话机制问题漏洞	CNNVD-2026-25492173	CVE-2026-81268	高危	https://www.ibm.com/support/pages/node/7286662	IBM
107	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-71110029	CVE-2026-81265	高危	https://www.ibm.com/support/pages/node/7286665	IBM
108	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-87372285	CVE-2026-81213	高危	https://www.ibm.com/support/pages/node/7286665	IBM
109	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-21715245	CVE-2026-81211	高危	https://www.ibm.com/support/pages/node/7286666	IBM
110	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-45533613	CVE-2026-79742	高危	https://www.ibm.com/support/pages/node/7286666	IBM
111	IBM Langflow OSS 命令注入漏洞	CNNVD-2026-48065931	CVE-2026-78575	高危	https://www.ibm.com/support/pages/node/7286666	IBM

112	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-60505010	CVE-2026-78571	高危	https://www.ibm.com/support/pages/node/7286666	IBM
113	IBM Langflow OSS 命令注入漏洞	CNNVD-2026-98621273	CVE-2026-78569	高危	https://www.ibm.com/support/pages/node/7286666	IBM
114	IBM Langflow OSS 处理逻辑错误漏洞	CNNVD-2026-77168685	CVE-2026-76059	高危	https://www.ibm.com/support/pages/node/7286666	IBM
115	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-18015475	CVE-2026-19306	高危	https://www.ibm.com/support/pages/node/7285641	IBM
116	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-34824189	CVE-2026-19304	高危	https://www.ibm.com/support/pages/node/7285639	IBM
117	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-42580461	CVE-2026-19305	高危	https://www.ibm.com/support/pages/node/7285639	IBM
118	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-32481590	CVE-2026-19303	高危	https://www.ibm.com/support/pages/node/7285643	IBM
119	IBM Langflow OSS 信息泄露漏洞	CNNVD-2026-19719373	CVE-2026-19300	高危	https://www.ibm.com/support/pages/node/7285642	IBM
120	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-60331786	CVE-2026-19298	高危	https://www.ibm.com/support/pages/node/7285640	IBM
121	IBM Langflow OSS 路径遍历漏	CNNVD-2026-92930890	CVE-2026-84889	高危	https://www.ibm.com/su	IBM

	洞				pport/pages/node/7286656	
122	IBM Langflow OSS 权限许可和访问控制问题漏洞	CNNVD-2026-84955899	CVE-2026-81941	高危	https://www.ibm.com/support/pages/node/7286666	IBM
123	IBM Langflow OSS 代码注入漏洞	CNNVD-2026-44390810	CVE-2026-81940	高危	https://www.ibm.com/support/pages/node/7286666	IBM
124	ihor-sokoliuk mcp-searxng 服务端请求伪造漏洞	CNNVD-2026-89045128	CVE-2026-58485	高危	https://github.com/ihor-sokoliuk/mcp-searxng/releases/tag/v1.7.1	ihor-sokoliuk
125	ihor-sokoliuk mcp-searxng 资源管理错误漏洞	CNNVD-2026-91608285	CVE-2026-58483	高危	https://github.com/ihor-sokoliuk/mcp-searxng/releases/tag/v1.7.1	ihor-sokoliuk
126	Interinfo DreamMaker SQL 注入漏洞	CNNVD-2026-46755121	CVE-2026-85540	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。	Interinfo
127	InternLM LMDeploy 资源管理错误漏洞	CNNVD-2026-76605400	CVE-2026-33625	高危	https://github.com/InternLM/lmdeploy	InternLM
128	InternLM LMDeploy 资源管理错误漏洞	CNNVD-2026-50532248	CVE-2026-92983	高危	目前厂商暂未发布修复措施解决此	InternLM

					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。	
129	InternLM LMDeploy 异常处理不当漏洞	CNNVD-2026-34290884	CVE-2026-92971	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。	InternLM
130	Ivanti Sentry 授权问题漏洞	CNNVD-2026-28468120	CVE-2026-83527	高危	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2026-83527	Ivanti
131	Jina AI Reader 服务端请求伪造漏洞	CNNVD-2026-30712074	CVE-2026-85699	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。	Jina AI
132	Jupyter Notebook Viewer 路径遍历漏洞	CNNVD-2026-73234941	CVE-2026-86258	高危	https://github.com/jupyter/nbviewer/commit/aad36106f72a1ca7721310c6fccc677ce4c744a5	Jupyter
133	LangBot 授权问	CNNVD-2026-	CVE-2026-	高危	https://git	LangBot

	题漏洞	87571282	90938		hub.com/langbot-app/LangBot/security/advisories/GHSA-m7qm-2mjr-2h4q	
134	Lenovo Tianxi AI Agent PC Application 命令注入漏洞	CNNVD-2026-51111282	CVE-2026-19136	高危	https://iknow.lenovo.com.cn/detail/442249	Lenovo
135	lightgbm-org Light Gradient Boosting Machine 缓冲区错误漏洞	CNNVD-2026-83671501	CVE-2026-92786	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。	lightgbm-org
136	llmware.ai llmware SQL 注入漏洞	CNNVD-2026-59594479	CVE-2026-85689	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。	llmware.ai
137	Maxim AI Bifrost AI Gateway 权限许可和访问控制问题漏洞	CNNVD-2026-39682802	CVE-2026-86242	高危	https://github.com/maximhq/bifrost/releases/tag/transports/v2.0.0	Maxim AI
138	Mervin Praison PraisonAI 处理逻辑错误漏洞	CNNVD-2026-23948362	CVE-2026-57137	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-h2w2-v7j6-xqm4	Mervin Praison

139	Mervin Praison PraisonAI 处理逻辑错误漏洞	CNNVD-2026-43781200	CVE-2026-57136	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-vjv9-7m7j-h833	Mervin Praison
140	Mervin Praison PraisonAI 权限许可和访问控制问题漏洞	CNNVD-2026-88947171	CVE-2026-57135	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-gqmf-56h7-rrpf	Mervin Praison
141	Mervin Praison PraisonAI 处理逻辑错误漏洞	CNNVD-2026-90745096	CVE-2026-57133	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-5jv7-2mjm-h6qj	Mervin Praison
142	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-21834597	CVE-2026-57134	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-4qq2-2j2x-x62c	Mervin Praison
143	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-13804130	CVE-2026-57112	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-vmf9-xx9w-86wx	Mervin Praison
144	Mervin Praison PraisonAI 路径遍历漏洞	CNNVD-2026-78791635	CVE-2026-57129	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-2rcg-	Mervin Praison

					mm5h-xchx	
145	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-26755605	CVE-2026-57132	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-8ccj-p46r-jwqq	Mervin Praison
146	Mervin Praison PraisonAI 输入验证错误漏洞	CNNVD-2026-64566824	CVE-2026-57130	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-c969-5x3p-vq3v	Mervin Praison
147	Mervin Praison PraisonAI 服务端请求伪造漏洞	CNNVD-2026-77486762	CVE-2026-57126	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-vxgj-xg5c-p4h7	Mervin Praison
148	Mervin Praison PraisonAI 输入验证错误漏洞	CNNVD-2026-20185836	CVE-2026-57122	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-x92v-rpx6-p6cw	Mervin Praison
149	Mervin Praison PraisonAI 路径遍历漏洞	CNNVD-2026-56597900	CVE-2026-57119	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-p4pj-vh7h-6cqh	Mervin Praison
150	Mervin Praison PraisonAI 信息泄露漏洞	CNNVD-2026-87284634	CVE-2026-56839	高危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHS	Mervin Praison

					A-gcq3-mfvh-3x25	
151	Microsoft Azure Machine Learning 授权问题漏洞	CNNVD-2026-11283524	CVE-2026-68791	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68791	Microsoft
152	Microsoft Windows ML CLI 授权问题漏洞	CNNVD-2026-46145601	CVE-2026-84452	高危	https://github.com/microsoft/winml-cli/security/advisories/GHSA-96p9-rh4f-92cf	Microsoft
153	Microsoft Azure AI Foundry 服务端请求伪造漏洞	CNNVD-2026-26347433	CVE-2026-85917	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-85917	Microsoft
154	Microsoft Fabric 授权问题漏洞	CNNVD-2026-51015698	CVE-2026-70178	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-70178	Microsoft
155	Microsoft Discovery Studio 输入验证错误漏洞	CNNVD-2026-47948241	CVE-2026-62906	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62906	Microsoft
156	MindsDB 服务端请求伪造漏洞	CNNVD-2026-35584345	CVE-2026-86173	高危	目前厂商暂未发布修复措施解决此安全问题，	MindsDB

					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。	
157	Mistral AI Mistral Vibe 软件供应链问题漏洞	CNNVD-2026-91173155	CVE-2026-93993	高危	https://github.com/mistralai/mistral-vibe/releases/tag/v2.25.5	Mistral AI
158	MLflow 反序列化注入漏洞	CNNVD-2026-79076520	CVE-2026-96804	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。	MLflow
159	MLflow 反序列化注入漏洞	CNNVD-2026-86788906	CVE-2026-96775	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。	MLflow
160	MLflow 软件供应链问题漏洞	CNNVD-2026-12266582	CVE-2026-79721	高危	https://github.com/mlflow/mlflow	MLflow
161	ModelScope ms-swift 服务端请求伪造漏洞	CNNVD-2026-18578413	CVE-2026-85686	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	ModelScope

					考网址以获取解决办法。	
162	Murtaza Nasir Speakr 授权问题漏洞	CNNVD-2026-38428231	CVE-2026-54510	高危	https://github.com/murtaza-nasir/speakr/security/advisories/GHSA-x4q4-3ww4-h329	Murtaza Nasir
163	naranor agent-coderag 命令注入漏洞	CNNVD-2026-73659363	CVE-2026-57586	高危	https://github.com/naranor/agent-coderag/security/advisories/GHSA-wg5p-8h9p-3mr7	naranor
164	NetEase QAnything 授权问题漏洞	CNNVD-2026-38432055	CVE-2026-85671	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。	NetEase
165	NousResearch Hermes Agent 命令注入漏洞	CNNVD-2026-15385881	CVE-2026-71963	高危	https://github.com/NousResearch/hermes-agent/pull/101483	NousResearch
166	NVIDIA Triton Inference Server 授权问题漏洞	CNNVD-2026-45281258	CVE-2026-47625	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。	NVIDIA

167	NVIDIA NeMo Speech 反序列化注入漏洞	CNNVD-2026-55034667	CVE-2026-65179	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。	NVIDIA
168	NVIDIA NeMo Speech 反序列化注入漏洞	CNNVD-2026-96596014	CVE-2026-65178	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。	NVIDIA
169	NVIDIA NeMo Speech 命令注入漏洞	CNNVD-2026-43172073	CVE-2026-65111	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。	NVIDIA
170	NVIDIA Triton Inference Server 资源管理错误漏洞	CNNVD-2026-47812134	CVE-2026-16497	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。	NVIDIA
171	NVIDIA NeMo Speech 反序列化注入漏洞	CNNVD-2026-21677982	CVE-2026-24239	高危	目前厂商暂未发布修复措施解决此	NVIDIA

					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。	
172	NVIDIA NeMo Speech 反序列化注入漏洞	CNNVD-2026-91490467	CVE-2026-24267	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。	NVIDIA
173	ogx-ai OGX 服务端请求伪造漏洞	CNNVD-2026-41006139	CVE-2026-85666	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。	ogx-ai
174	Ollama 服务端请求伪造漏洞	CNNVD-2026-94820222	CVE-2026-85180	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。	Ollama
175	Onyx 信任管理问题漏洞	CNNVD-2026-40312330	CVE-2026-85700	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	Onyx

					随时关注厂商主页或参考网址以获取解决办法。	
176	OpenC3 COSMOS 命令注入漏洞	CNNVD-2026-91522025	CVE-2026-77601	高危	https://github.com/OpenC3/cosmos/security/advisories/GHSA-vp3w-52v9-q57f	OpenC3
177	OpenC3 COSMOS 跨站脚本漏洞	CNNVD-2026-60862925	CVE-2026-77394	高危	https://github.com/OpenC3/cosmos/security/advisories/GHSA-gvf2-2rh5-mpgf	OpenC3
178	OpenClaw 输入验证错误漏洞	CNNVD-2026-27697311	CVE-2026-100598	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-r88x-r7jj-f2cf	OpenClaw
179	OpenClaw 命令注入漏洞	CNNVD-2026-73451451	CVE-2026-100599	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-224w-vfr9-h35c	OpenClaw
180	OpenClaw 竞争条件问题漏洞	CNNVD-2026-64413279	CVE-2026-100597	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-crg9-c62w-j2p5	OpenClaw
181	OpenClaw 授权问题漏洞	CNNVD-2026-28009648	CVE-2026-100596	高危	https://github.com/openclaw/openclaw/securit	OpenClaw

					y/advisories/GHSA-wwx7-573h-pqwc	
182	OpenClaw 授权问题漏洞	CNNVD-2026-64039546	CVE-2026-100588	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-jghr-xp78-995p	OpenClaw
183	OpenClaw 信息泄露漏洞	CNNVD-2026-12697602	CVE-2026-100595	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-4hwv-rj92-h7rp	OpenClaw
184	OpenClaw 信息泄露漏洞	CNNVD-2026-80410959	CVE-2026-100594	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-89cw-7452-cfrf	OpenClaw
185	OpenClaw 授权问题漏洞	CNNVD-2026-90237574	CVE-2026-100589	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-9x88-f7rh-4c83	OpenClaw
186	OpenClaw 授权问题漏洞	CNNVD-2026-15557360	CVE-2026-100587	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-pjjr-5qhr-5w6r	OpenClaw
187	OpenClaw 授权问题漏洞	CNNVD-2026-52529950	CVE-2026-100585	高危	https://github.com/openclaw/openc	OpenClaw

					law/security/advisories/GHSA-p5g8-m35v-7m82	
188	OpenClaw 权限许可和访问控制问题漏洞	CNNVD-2026-82552542	CVE-2026-100586	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-9p6m-2872-xm7x	OpenClaw
189	OpenClaw 输入验证错误漏洞	CNNVD-2026-36576154	CVE-2026-100580	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-8xxh-v4vc-qvm4	OpenClaw
190	OpenClaw 授权问题漏洞	CNNVD-2026-12019321	CVE-2026-100579	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-4wvr-f35r-f8w4	OpenClaw
191	OpenClaw 权限许可和访问控制问题漏洞	CNNVD-2026-49196326	CVE-2026-100578	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-qw7m-h363-33qw	OpenClaw
192	OpenClaw 授权问题漏洞	CNNVD-2026-61270462	CVE-2026-100575	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-58qx-6m8p-wh2j	OpenClaw
193	OpenClaw 服务端请求伪造漏洞	CNNVD-2026-49731732	CVE-2026-100574	高危	https://github.com/ope	OpenClaw

					nclaw/openclaw/security/advisories/GHSA-72p2-79fg-pvph	
194	OpenClaw 命令注入漏洞	CNNVD-2026-79541135	CVE-2026-100570	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-5mrc-77hj-xjxv	OpenClaw
195	OpenClaw 服务端请求伪造漏洞	CNNVD-2026-38264404	CVE-2026-100567	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-p3h6-v2h4-36q2	OpenClaw
196	OpenClaw 命令注入漏洞	CNNVD-2026-33308257	CVE-2026-100561	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-ghpx-6xwq-2w4w	OpenClaw
197	OpenClaw 信息泄露漏洞	CNNVD-2026-48822233	CVE-2026-100568	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-hpg5-cq3m-phqp	OpenClaw
198	OpenClaw 服务端请求伪造漏洞	CNNVD-2026-83266358	CVE-2026-100555	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-cf95-m4jv-59rc	OpenClaw
199	OpenClaw 授权	CNNVD-2026-	CVE-2026-	高危	https://git	OpenClaw

	问题漏洞	62835562	100560		hub.com/openclaw/openclaw/security/advisories/GHSA-74gc-hg2m-79p9	
200	OpenClaw 命令注入漏洞	CNNVD-2026-54008690	CVE-2026-100559	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-9f86-pvv5-rxfw	OpenClaw
201	OpenClaw 资源管理错误漏洞	CNNVD-2026-50909476	CVE-2026-100558	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-4r25-35qc-fr6j	OpenClaw
202	OpenClaw 授权问题漏洞	CNNVD-2026-81971346	CVE-2026-100557	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-7cp7-87pj-p32v	OpenClaw
203	OpenClaw 授权问题漏洞	CNNVD-2026-73404594	CVE-2026-100552	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-wwcw-jfpp-gpxw	OpenClaw
204	OpenClaw 信息泄露漏洞	CNNVD-2026-99339635	CVE-2026-100543	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-qgj5-6x35-9g6f	OpenClaw

205	OpenClaw 授权问题漏洞	CNNVD-2026-71652530	CVE-2026-100538	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-w5x7-c87m-3jpc	OpenClaw
206	OpenClaw 授权问题漏洞	CNNVD-2026-19221655	CVE-2026-100535	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-62qm-6fjj-6g23	OpenClaw
207	OpenClaw 授权问题漏洞	CNNVD-2026-23063626	CVE-2026-100531	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-v7hh-7676-rg67	OpenClaw
208	OpenClaw 路径遍历漏洞	CNNVD-2026-51311013	CVE-2026-100536	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-fphf-69cp-h5xw	OpenClaw
209	OpenClaw 授权问题漏洞	CNNVD-2026-78928676	CVE-2026-100530	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-3mq7-q27j-mq7q	OpenClaw
210	OpenClaw 授权问题漏洞	CNNVD-2026-12883592	CVE-2026-100529	高危	https://github.com/openclaw/openclaw/security/advisories/GHSA-7jfq-rmfm-	OpenClaw

					29wp	
211	plandex-ai plandex 路径遍历漏洞	CNNVD-2026-59083791	CVE-2026-85690	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。	plandex-ai
212	Polyaxon 代码注入漏洞	CNNVD-2026-61627792	CVE-2026-91925	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。	polyaxon
213	potpie.ai potpie 授权问题漏洞	CNNVD-2026-96899161	CVE-2026-85669	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。	potpie.ai
214	Project MONAI MONAI 反序列化注入漏洞	CNNVD-2026-25049124	CVE-2026-100846	高危	https://github.com/Project-MONAI/MONAI/security/advisories/GHSA-89gg-p5r5-q6r4	Project MONAI
215	Project MONAI MONAI 命令注入漏洞	CNNVD-2026-25250839	CVE-2026-100844	高危	https://github.com/Project-MONAI/MONAI/security/a	Project MONAI

					dvisories/GHSA-rghg-q7wp-9767	
216	Project MONAI MONAI 反序列化注入漏洞	CNNVD-2026-87934757	CVE-2026-100845	高危	https://github.com/Project-MONAI/MONAI/security/advisories/GHSA-wg9g-w2j2-8pgr	Project MONAI
217	Project MONAI MONAI 反序列化注入漏洞	CNNVD-2026-37863549	CVE-2026-100843	高危	https://github.com/Project-MONAI/MONAI/security/advisories/GHSA-qxq5-qhx6-94qw	Project MONAI
218	Project MONAI MONAI 代码注入漏洞	CNNVD-2026-46403206	CVE-2026-100842	高危	https://github.com/Project-MONAI/MONAI/security/advisories/GHSA-h89g-r5pc-wxfm	Project MONAI
219	Project MONAI MONAI 反序列化注入漏洞	CNNVD-2026-19942671	CVE-2026-100841	高危	https://github.com/Project-MONAI/MONAI/security/advisories/GHSA-636w-j999-g7x5	Project MONAI
220	Project MONAI MONAI 代码注入漏洞	CNNVD-2026-25951395	CVE-2026-100840	高危	https://github.com/Project-MONAI/MONAI/security/advisories/GHSA-873f-pvrv-4x83	Project MONAI
221	RooCodeInc Roo Code 输入验证错误漏洞	CNNVD-2026-92418716	CVE-2026-82536	高危	目前厂商暂未发布修复措施解决此安全问题，	Roomote

					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。	
222	RooCodeInc Roo Code 处理逻辑错误漏洞	CNNVD-2026-54212319	CVE-2026-82537	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
223	SciPhi-AI R2R SQL 注入漏洞	CNNVD-2026-93276038	CVE-2026-82527	高危	https://github.com/SciPhi-AI/R2R/issues/2308	SciPhi-AI
224	sgl-project sglang 资源管理错误漏洞	CNNVD-2026-90747446	CVE-2026-93838	高危	https://github.com/sgl-project/sglang/releases	sgl-project
225	sgl-project sglang 资源管理错误漏洞	CNNVD-2026-15087564	CVE-2026-93688	高危	https://github.com/sgl-project/sglang/releases	sgl-project
226	sgl-project sglang 授权问题漏洞	CNNVD-2026-21124517	CVE-2026-92972	高危	https://github.com/sgl-project/sglang/releases	sgl-project
227	Stacklok ToolHive 权限许可和访问控制问题漏洞	CNNVD-2026-91773100	CVE-2026-58197	高危	https://github.com/stacklok/toolhive/security/advisories/GHSA-	Stacklok

					qg2g-g9w3-m5h8	
228	StacklokLabs MKP 资源管理错误漏洞	CNNVD-2026-71579690	CVE-2026-50125	高危	https://github.com/StacklokLabs/mkp/security/advisories/GHSA-qw5r-ppcg-f8rj	StacklokLabs
229	Stanford NLP Stanza 路径遍历漏洞	CNNVD-2026-85537776	CVE-2026-59974	高危	https://github.com/stanfordnlp/stanza/security/advisories/GHSA-2fwf-f686-7p34	Stanford NLP
230	Tencent WeKnora 服务端请求伪造漏洞	CNNVD-2026-88818381	CVE-2026-91750	高危	https://github.com/Tencent/WeKnora/releases	Tencent
231	Tencent AI-Infra-Guard 处理逻辑错误漏洞	CNNVD-2026-10930200	CVE-2026-84809	高危	https://github.com/Tencent/AI-Infra-Guard/commit/7e0f749e3c023e5c6ab7b32fe97b3f6f2e8aeb04	Tencent
232	tesseract-ocr Tesseract 缓冲区错误漏洞	CNNVD-2026-94565784	CVE-2026-88053	高危	https://github.com/tesseract-ocr/tesseract/security/advisories/GHSA-rphx-x795-5qjv	tesseract-ocr
233	tesseract-ocr Tesseract 输入验证错误漏洞	CNNVD-2026-49996417	CVE-2026-88052	高危	https://github.com/tesseract-ocr/tesseract/security/advisories/GHSA-2hm8-q5c7-c373	tesseract-ocr
234	tesseract-ocr	CNNVD-2026-	CVE-2026-	高危	https://git	tesseract

	Tesseract 缓冲区错误漏洞	77461648	88051		hub.com/tesseract-ocr/tesseract/security/advisories/GHSA-88qp-4g94-3rf3	-ocr
235	tesseract-ocr Tesseract 缓冲区错误漏洞	CNNVD-2026-20704862	CVE-2026-88049	高危	https://github.com/tesseract-ocr/tesseract/security/advisories/GHSA-jgq8-pprg-vc68	tesseract-ocr
236	tesseract-ocr Tesseract 缓冲区错误漏洞	CNNVD-2026-37744762	CVE-2026-88047	高危	https://github.com/tesseract-ocr/tesseract/security/advisories/GHSA-5j2p-r5vc-q7f3	tesseract-ocr
237	tesseract-ocr Tesseract 缓冲区错误漏洞	CNNVD-2026-31562761	CVE-2026-88048	高危	https://github.com/tesseract-ocr/tesseract/security/advisories/GHSA-q44c-23p6-5mw6	tesseract-ocr
238	Vedant Deshpande AI Agent Automation 授权问题漏洞	CNNVD-2026-24924117	CVE-2026-54519	高危	https://github.com/vmDeshpande/ai-agent-automation/security/advisories/GHSA-qv97-83w4-ff86	Vedant Deshpande
239	Vedant Deshpande AI Agent Automation 路径遍历漏洞	CNNVD-2026-71891194	CVE-2026-54520	高危	https://github.com/vmDeshpande/ai-agent-automation/security/advisories/GH	Vedant Deshpande

					SA-cm8g-8jfq-887p	
240	vLLM 资源管理错误漏洞	CNNVD-2026-68582058	CVE-2026-94627	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。	vLLM
241	vLLM 资源管理错误漏洞	CNNVD-2026-44014636	CVE-2026-94626	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。	vLLM
242	vLLM 资源管理错误漏洞	CNNVD-2026-24780005	CVE-2026-94624	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。	vLLM
243	vLLM 异常处理不当漏洞	CNNVD-2026-52367828	CVE-2026-94623	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。	vLLM
244	vLLM 异常处理	CNNVD-2026-	CVE-2026-	高危	目前厂商暂	vLLM

	不当漏洞	44361384	94622		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。	
245	vLLM 资源管理错误漏洞	CNNVD-2026-37764653	CVE-2026-93436	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。	vLLM
246	vLLM 输入验证错误漏洞	CNNVD-2026-30641656	CVE-2026-93592	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-25q3-v2hm-8vpf	vLLM
247	vLLM 代码注入漏洞	CNNVD-2026-86351648	CVE-2026-90553	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-3c86-2m5g-59q7	vLLM
248	vLLM 资源管理错误漏洞	CNNVD-2026-98830536	CVE-2026-90555	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-99f2-hwrc-gvq8	vLLM
249	vLLM 资源管理错误漏洞	CNNVD-2026-98047107	CVE-2026-100650	高危	https://github.com/vll	vLLM

					m-project/vllm/security/advisories/GHSA-p6g9-7v3x-m8mv	
250	vLLM 信任管理问题漏洞	CNNVD-2026-82837092	CVE-2026-100653	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-hhv2-872h-628q	vLLM
251	vLLM 输入验证错误漏洞	CNNVD-2026-97617273	CVE-2026-100654	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-v5gm-qgmv-gc6c	vLLM
252	vLLM 输入验证错误漏洞	CNNVD-2026-12809108	CVE-2026-100652	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-qff2-492f-9fm4	vLLM
253	vLLM 资源管理错误漏洞	CNNVD-2026-86721431	CVE-2026-100651	高危	https://github.com/vllm-project/vllm/security/advisories/GHSA-3mqx-f33v-vgp9	vLLM
254	Weights & Biases wandb 路径遍历漏洞	CNNVD-2026-61747080	CVE-2026-91771	高危	https://github.com/wandb/wandb/releases/tag/v0.29.0	Weights & Biases
255	WordPress Agentimus 授权问题漏洞	CNNVD-2026-74776338	CVE-2026-84779	高危	https://wordpress.org/plugins/agentimus/	WordPress

256	Xorbits Inference 输入验证错误漏洞	CNNVD-2026-28775388	CVE-2026-85668	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。	Xorbits
257	Yaowei Zheng LlamaFactory 服务端请求伪造漏洞	CNNVD-2026-95018598	CVE-2026-85673	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。	Yaowei Zheng
258	1MillionBot AI Chatbot Platform 跨站脚本漏洞	CNNVD-2026-39740359	CVE-2026-91921	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。	1MillionBot
259	Amazon Agent Toolkit for AWS 权限许可和访问控制问题漏洞	CNNVD-2026-77496656	CVE-2026-87912	中危	https://github.com/aws/agent-toolkit-for-aws/security/advisories/GHSA-2px6-hhjp-3g5x	Amazon
260	Anil Chandra Naidu Matcha Open Generative AI	CNNVD-2026-29064948	CVE-2026-90602	中危	目前厂商暂未发布修复措施解决此安全问题，	Anil Chandra Naidu Matcha

	跨站脚本漏洞				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。	
261	Ash Framework Ash AI 权限许可和访问控制问题漏洞	CNNVD-2026-83623659	CVE-2026-78230	中危	https://github.com/ash-project/ash_ai/security/advisories/GHSA-v5rw-36x5-r5vx	Ash Framework
262	BerriAI LiteLLM 服务端请求伪造漏洞	CNNVD-2026-40710406	CVE-2026-84377	中危	https://github.com/BerriAI/litellm/security/advisories/GHSA-3cv6-jpf6-8222	BerriAI
263	BerriAI LiteLLM 服务端请求伪造漏洞	CNNVD-2026-45507158	CVE-2026-59823	中危	https://github.com/BerriAI/litellm/security/advisories/GHSA-hx8v-g79f-8w5f	BerriAI
264	Cheshire Cat AI 授权问题漏洞	CNNVD-2026-80006010	CVE-2026-90579	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
265	CMU Sphinx PocketSphinx 缓冲区错误漏洞	CNNVD-2026-79765142	CVE-2026-54559	中危	https://github.com/cmusphinx/pocketsphinx/security/advisories/GHSA	CMU Sphinx

					-56r5-2p2f-7cxp	
266	Data Intelligence Lab@HKU nanobot 输入验证错误漏洞	CNNVD-2026-54154786	CVE-2026-90808	中危	https://github.com/HKUDS/nanobot/commit/af582246f141311d574551b7571a517bcc3df750	Data Intelligence Lab@HKU
267	Data Intelligence Lab@HKU nanobot 输入验证错误漏洞	CNNVD-2026-62413027	CVE-2026-90809	中危	https://github.com/HKUDS/nanobot/commit/af582246f141311d574551b7571a517bcc3df750	Data Intelligence Lab@HKU
268	Data Intelligence Lab@HKU LightRAG 跨站脚本漏洞	CNNVD-2026-93935926	CVE-2026-86062	中危	https://github.com/HKUDS/LightRAG/security/advisories/GHSA-xpjq-3w4w-w5wr	Data Intelligence Lab@HKU
269	Data Intelligence Lab@HKU LightRAG 侧信道信息泄露漏洞	CNNVD-2026-21310290	CVE-2026-85725	中危	https://github.com/HKUDS/LightRAG/security/advisories/GHSA-c759-cx9p-mrwq	Data Intelligence Lab@HKU
270	Data Intelligence Lab@HKU LightRAG 信息泄露漏洞	CNNVD-2026-78338619	CVE-2026-85709	中危	https://github.com/HKUDS/LightRAG/security/advisories/GHSA-hrmj-7rvj-4hg8	Data Intelligence Lab@HKU
271	decolua 9Router 授权问题漏洞	CNNVD-2026-69854379	CVE-2026-56682	中危	https://github.com/decolua/9router/security/advisories/GHSA-32gc-64m7-hj7v	decolua
272	Discourse 输入	CNNVD-2026-	CVE-2026-	中危	https://git	Discourse

	验证错误漏洞	28419612	91134		hub.com/discourse/discourse/security/advisories/GHSA-54vw-chv3-wjpv	
273	Discourse 输入验证错误漏洞	CNNVD-2026-60265385	CVE-2026-91132	中危	https://github.com/discourse/discourse/security/advisories/GHSA-4q3q-hph3-3rvp	Discourse
274	Discourse 输入验证错误漏洞	CNNVD-2026-87558074	CVE-2026-91133	中危	https://github.com/discourse/discourse/security/advisories/GHSA-8hxh-573g-52gx	Discourse
275	Discourse 跨站脚本漏洞	CNNVD-2026-88823199	CVE-2026-91121	中危	https://github.com/discourse/discourse/security/advisories/GHSA-34rh-wjfv-65gq	Discourse
276	Discourse 跨站脚本漏洞	CNNVD-2026-36097578	CVE-2026-91120	中危	https://github.com/discourse/discourse/security/advisories/GHSA-h7cg-2vww-m45c	Discourse
277	Discourse 跨站脚本漏洞	CNNVD-2026-33287662	CVE-2026-91119	中危	https://github.com/discourse/discourse/security/advisories/GHSA-pv3p-p3m9-v8v3	Discourse

278	Discourse 授权问题漏洞	CNNVD-2026-12158554	CVE-2026-84302	中危	https://github.com/discourse/discourse/security/advisories/GHSA-3rx9-fqgh-wfpc	Discourse
279	Discourse 跨站脚本漏洞	CNNVD-2026-54418252	CVE-2026-59830	中危	https://github.com/discourse/discourse/security/advisories/GHSA-x6mf-p7cg-69rw	Discourse
280	FlowiseAI Flowise 授权问题漏洞	CNNVD-2026-76627772	CVE-2026-90535	中危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-xhxx-56g3-mx2r	FlowiseAI
281	FlowiseAI Flowise 授权问题漏洞	CNNVD-2026-83142831	CVE-2026-90534	中危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-hqvm-7539-v83j	FlowiseAI
282	FlowiseAI Flowise 授权问题漏洞	CNNVD-2026-39744008	CVE-2026-90533	中危	https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-fhxm-xxcx-g6x3	FlowiseAI
283	ggml llama.cpp 异常处理不当漏洞	CNNVD-2026-46446947	CVE-2026-86317	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	ggml

					商主页或参考网址以获取解决办法。	
284	Hubcore.ai HubCore 安全漏洞	CNNVD-2026-52051124	CVE-2026-75170	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。	Hubcore.ai
285	Hubcore.ai HubCore 安全漏洞	CNNVD-2026-86566000	CVE-2026-75171	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。	Hubcore.ai
286	IBM Langflow OSS 权限许可和访问控制问题漏洞	CNNVD-2026-91270902	CVE-2026-79725	中危	https://www.ibm.com/support/pages/node/7286657	IBM
287	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-51925160	CVE-2026-79723	中危	https://www.ibm.com/support/pages/node/7286665	IBM
288	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-28600248	CVE-2026-12767	中危	https://www.ibm.com/support/pages/node/7286665	IBM
289	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-23770677	CVE-2026-12765	中危	https://www.ibm.com/support/pages/node/7285644	IBM
290	IBM Langflow	CNNVD-2026-	CVE-2026-	中危	https://www	IBM

	OSS 服务端请求伪造漏洞	40783413	12766		.ibm.com/support/pages/node/7285639	
291	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-51424884	CVE-2026-12763	中危	https://www.ibm.com/support/pages/node/7286662	IBM
292	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-59200293	CVE-2026-17628	中危	https://www.ibm.com/support/pages/node/7286684	IBM
293	IBM Langflow OSS 跨站脚本漏洞	CNNVD-2026-11470637	CVE-2026-8447	中危	https://www.ibm.com/support/pages/node/7285646	IBM
294	IBM MQ Agent 资源管理错误漏洞	CNNVD-2026-91062748	CVE-2026-19645	中危	https://www.ibm.com/support/pages/node/7285394	IBM
295	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-28330265	CVE-2026-19302	中危	https://www.ibm.com/support/pages/node/7285641	IBM
296	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-55894037	CVE-2026-19301	中危	https://www.ibm.com/support/pages/node/7285639	IBM
297	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-13288661	CVE-2026-19299	中危	https://www.ibm.com/support/pages/node/7285641	IBM
298	IBM Langflow OSS 服务端请求伪造漏洞	CNNVD-2026-46742403	CVE-2026-17631	中危	https://www.ibm.com/support/pages/node/7285644	IBM
299	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-77820175	CVE-2026-17627	中危	https://www.ibm.com/support/pages	IBM

					/node/7286294	
300	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-67233821	CVE-2026-17621	中危	https://www.ibm.com/support/pages/node/7286293	IBM
301	IBM Cognos Analytics 跨站脚本漏洞	CNNVD-2026-27886999	CVE-2026-7884	中危	https://www.ibm.com/support/pages/node/7287209	IBM
302	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-67633727	CVE-2026-17622	中危	https://www.ibm.com/support/pages/node/7286293	IBM
303	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-42547172	CVE-2026-14470	中危	https://www.ibm.com/support/pages/node/7286293	IBM
304	IBM Langflow OSS 授权问题漏洞	CNNVD-2026-92752920	CVE-2026-9225	中危	https://www.ibm.com/support/pages/node/7286657	IBM
305	IBM Cognos Analytics 信息泄露漏洞	CNNVD-2026-47835253	CVE-2025-36076	中危	https://www.ibm.com/support/pages/node/7287209	IBM
306	IBM Cognos Analytics 加密问题漏洞	CNNVD-2026-66647675	CVE-2025-33147	中危	https://www.ibm.com/support/pages/node/7287209	IBM
307	IBM Cognos Analytics 加密问题漏洞	CNNVD-2026-52034986	CVE-2024-56344	中危	https://www.ibm.com/support/pages/node/7287211	IBM
308	IBM Langflow OSS 路径遍历漏洞	CNNVD-2026-97221078	CVE-2026-9138	中危	https://www.ibm.com/support/pages/node/7285643	IBM

309	IBM Langflow OSS 权限许可和访问控制问题漏洞	CNNVD-2026-69885430	CVE-2026-9186	中危	https://www.ibm.com/support/pages/node/7285646	IBM
310	IBM Qiskit SDK 反序列化注入漏洞	CNNVD-2026-94304180	CVE-2026-19795	中危	https://www.ibm.com/support/pages/node/7285932	IBM
311	iFLYTEK Astron Agent 服务端请求伪造漏洞	CNNVD-2026-78269225	CVE-2026-95930	中危	https://github.com/iflytek/astron-agent/commit/45ee5fb647e9894e73b0d7720fa94a66e4540bbb	iFLYTEK
312	iFLYTEK Astron Agent 输入验证错误漏洞	CNNVD-2026-35151120	CVE-2026-95929	中危	https://github.com/iflytek/astron-agent/commit/6702be70ae802b1048f5fbec91e690e7b71a4165	iFLYTEK
313	ihor-sokoliuk mcp-searxng 信息泄露漏洞	CNNVD-2026-32228378	CVE-2026-54689	中危	https://github.com/ihor-sokoliuk/mcp-searxng/releases/tag/v1.2.0	ihor-sokoliuk
314	ihor-sokoliuk mcp-searxng 服务端请求伪造漏洞	CNNVD-2026-25794640	CVE-2026-54688	中危	https://github.com/ihor-sokoliuk/mcp-searxng/releases/tag/v1.2.0	ihor-sokoliuk
315	InfiniFlow RAGFlow 路径遍历漏洞	CNNVD-2026-72679490	CVE-2026-93013	中危	目前厂商暂未发布修复措施解决此	InfiniFlow

					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。	
316	Interinfo DreamMaker 跨站脚本漏洞	CNNVD-2026-31253671	CVE-2026-85541	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。	Interinfo
317	labring FastGPT 服务端请求伪造漏洞	CNNVD-2026-96721180	CVE-2026-84301	中危	https://github.com/labring/FastGPT/security/advisories/GHSA-6jwp-qf29-hpj9	labring
318	LangChain langgraph-api 授权问题漏洞	CNNVD-2026-55664564	CVE-2026-55235	中危	https://github.com/langchain-ai/helm/security/advisories/GHSA-2c9q-c2q9-qgqv	LangChain
319	LobeHub 输入验证错误漏洞	CNNVD-2026-11245715	CVE-2026-85621	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。	LobeHub
320	Lovepreet Singh MCP	CNNVD-2026-88792367	CVE-2026-94044	中危	https://github.com/03-	Lovepreet Singh

	server setup guide 路径遍历漏洞				lovepreetSingh/MCP/issues/3	
321	Meesho BharatMLStack 安全漏洞	CNNVD-2026-22119698	CVE-2026-39040	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。	Meesho
322	Meesho BharatMLStack 安全漏洞	CNNVD-2026-44653087	CVE-2026-39038	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。	Meesho
323	Meesho BharatMLStack 安全漏洞	CNNVD-2026-59488455	CVE-2026-39039	中危	https://github.com/Meesho/BharatMLStack	Meesho
324	Mervin Praison PraisonAI 授权问题漏洞	CNNVD-2026-58959790	CVE-2026-57128	中危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-35w5-pcw4-jx94	Mervin Praison
325	Mervin Praison PraisonAI 处理逻辑错误漏洞	CNNVD-2026-68324080	CVE-2026-57120	中危	https://github.com/MervinPraison/PraisonAI/security/advisories/GHSA-pv2j-rghr-v5r9	Mervin Praison
326	Mervin Praison PraisonAI 服务	CNNVD-2026-30358044	CVE-2026-57115	中危	https://github.com/Mer	Mervin Praison

	端请求伪造漏洞				vinPraison/PraisonAI/security/advisories/GHSA-6h9p-93hq-q7h6	
327	Microsoft Copilot 命令注入漏洞	CNNVD-2026-90585589	CVE-2026-55946	中危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-55946	Microsoft
328	Mintplex Labs AnythingLLM 跨站脚本漏洞	CNNVD-2026-59548718	CVE-2026-88055	中危	https://github.com/Mintplex-Labs/anything-llm/security/advisories/GHSA-rh3m-xv7m-9jhf	Mintplex Labs
329	MLRun 服务端请求伪造漏洞	CNNVD-2026-33379336	CVE-2026-92568	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。	MLRun
330	Moonshot AI Kimi AI 跨站脚本漏洞	CNNVD-2026-59772505	CVE-2026-79294	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。	Moonshot AI
331	NousResearch	CNNVD-2026-	CVE-2026-	中危	目前厂商暂	NousResea

	Hermes Agent 资源管理错误漏洞	47258700	85107		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。	rch
332	NousResearch Hermes Agent 服务端请求伪造漏洞	CNNVD-2026-93882791	CVE-2026-85106	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。	NousResearch
333	NousResearch Hermes Agent 授权问题漏洞	CNNVD-2026-18321851	CVE-2026-85105	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。	NousResearch
334	onData CKAN MCP Server 服务端请求伪造漏洞	CNNVD-2026-67132519	CVE-2026-61612	中危	https://github.com/ondata/ckan-mcp-server/security/advisories/GHSA-798p-78g2-v556	onData
335	openagents-org OpenAgents 服务端请求伪造漏洞	CNNVD-2026-69031662	CVE-2026-86237	中危	https://github.com/openagents-org/openagents/releases	openagents-org

336	OpenClaw 授权问题漏洞	CNNVD-2026-87025363	CVE-2026-100593	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-q9j5-4xr6-xqqw	OpenClaw
337	OpenClaw 授权问题漏洞	CNNVD-2026-20155721	CVE-2026-100592	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-22v4-33m3-8p7m	OpenClaw
338	OpenClaw 授权问题漏洞	CNNVD-2026-72060591	CVE-2026-100591	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-xw9g-7xvv-gcjc	OpenClaw
339	OpenClaw 授权问题漏洞	CNNVD-2026-81312181	CVE-2026-100590	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-5j27-v2pw-cj9m	OpenClaw
340	OpenClaw 加密问题漏洞	CNNVD-2026-60750521	CVE-2026-100581	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-gcm4-fmcp-2f9r	OpenClaw
341	OpenClaw 权限许可和访问控制问题漏洞	CNNVD-2026-60287037	CVE-2026-100584	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-rgjw-6v73-	OpenClaw

					php6	
342	OpenClaw 服务端请求伪造漏洞	CNNVD-2026-49096865	CVE-2026-100577	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-fvxr-9g24-x3hf	OpenClaw
343	OpenClaw 服务端请求伪造漏洞	CNNVD-2026-33363170	CVE-2026-100576	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-4g58-43jr-6738	OpenClaw
344	OpenClaw 资源管理错误漏洞	CNNVD-2026-80838310	CVE-2026-100571	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-xw48-j584-r73h	OpenClaw
345	OpenClaw 资源管理错误漏洞	CNNVD-2026-71478922	CVE-2026-100572	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-fw6q-2frm-jxxr	OpenClaw
346	OpenClaw 授权问题漏洞	CNNVD-2026-51955620	CVE-2026-100573	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-5m4g-88rg-69pj	OpenClaw
347	OpenClaw 信任管理问题漏洞	CNNVD-2026-15737260	CVE-2026-100569	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-	OpenClaw

					pfrw-r5vr-89hw	
348	OpenClaw 输入验证错误漏洞	CNNVD-2026-57357640	CVE-2026-100563	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-xx9p-hc9w-6p5h	OpenClaw
349	OpenClaw 输入验证错误漏洞	CNNVD-2026-19951907	CVE-2026-100564	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-39hf-qg99-f4qv	OpenClaw
350	OpenClaw 授权问题漏洞	CNNVD-2026-66846914	CVE-2026-100562	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-j4mm-p864-vx7f	OpenClaw
351	OpenClaw 授权问题漏洞	CNNVD-2026-62364555	CVE-2026-100556	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-mm7m-wcgh-8mfq	OpenClaw
352	OpenClaw 授权问题漏洞	CNNVD-2026-93779527	CVE-2026-100553	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-h9jh-75j7-7hhx	OpenClaw
353	OpenClaw 信息泄露漏洞	CNNVD-2026-89023947	CVE-2026-100548	中危	https://github.com/openclaw/openclaw/security/advisorie	OpenClaw

					s/GHSA-66hm-hxq3-5pfh	
354	OpenClaw 授权问题漏洞	CNNVD-2026-55432724	CVE-2026-100550	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-8938-r7c6-54vq	OpenClaw
355	OpenClaw 处理逻辑错误漏洞	CNNVD-2026-12466330	CVE-2026-100547	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-356g-m7rx-7pm3	OpenClaw
356	OpenClaw 路径遍历漏洞	CNNVD-2026-51510364	CVE-2026-100549	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-rm45-4jx5-2927	OpenClaw
357	OpenClaw 授权问题漏洞	CNNVD-2026-68036857	CVE-2026-100545	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-5fwv-rrvp-8xvr	OpenClaw
358	OpenClaw 竞争条件问题漏洞	CNNVD-2026-38088589	CVE-2026-100546	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-5x6q-wg56-rxg8	OpenClaw
359	OpenClaw 路径遍历漏洞	CNNVD-2026-18937644	CVE-2026-100533	中危	https://github.com/openclaw/openclaw/securit	OpenClaw

					y/advisories/GHSA-5rx7-34fw-64qg	
360	OpenClaw 信息泄露漏洞	CNNVD-2026-34325072	CVE-2026-100528	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-vhpg-cq3w-v8p9	OpenClaw
361	OpenClaw 资源管理错误漏洞	CNNVD-2026-17317377	CVE-2026-100527	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-m78m-7h3q-q938	OpenClaw
362	OpenClaw 授权问题漏洞	CNNVD-2026-91284298	CVE-2026-100525	中危	https://github.com/openclaw/openclaw/security/advisories/GHSA-rx8p-qcpv-c7vr	OpenClaw
363	ramon-victor FreeGPT WebUI 授权问题漏洞	CNNVD-2026-91776231	CVE-2026-85701	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。	ramon-victor
364	ramon-victor FreeGPT WebUI 授权问题漏洞	CNNVD-2026-53508127	CVE-2026-85702	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	ramon-victor

					考网址以获取解决办法。	
365	ramon-victor FreeGPT WebUI 资源管理错误漏洞	CNNVD-2026-74156035	CVE-2026-85703	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。	ramon-victor
366	REBUILD 安全漏洞	CNNVD-2026-91199697	CVE-2026-71802	中危	https://github.com/getrebuild/rebuild/releases	REBUILD
367	Refly AI Refly 服务端请求伪造漏洞	CNNVD-2026-28420588	CVE-2026-91199	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
368	RowBoat Labs rowboat 资源管理错误漏洞	CNNVD-2026-99975399	CVE-2026-84856	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。	RowBoat Labs
369	SAMSUNG Bixby Touch 权限许可和访问控制问题漏洞	CNNVD-2026-77649111	CVE-2026-21108	中危	https://security.samsungmobile.com/serviceWeb.smsb?year=2026&month	SAMSUNG

					=09	
370	SGLang 软件供应链问题漏洞	CNNVD-2026-23803298	CVE-2026-94570	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。	SGLang
371	SGLang 代码注入漏洞	CNNVD-2026-44557590	CVE-2026-86793	中危	https://github.com/sgl-project/sglang/releases	SGLang
372	simstudioai sim 服务端请求伪造漏洞	CNNVD-2026-13332958	CVE-2026-86115	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。	simstudioai
373	Simular Agent S 资源管理错误漏洞	CNNVD-2026-77997820	CVE-2026-84886	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。	Simular
374	Stacklok ToolHive 服务端请求伪造漏洞	CNNVD-2026-88052326	CVE-2026-58196	中危	https://github.com/stacklok/toolhive/security/advisories/GHSA-pr64-jmmf-	Stacklok

					jp54	
375	TensorOpera FEDML 输入验证错误漏洞	CNNVD-2026-14251311	CVE-2026-90614	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。	TensorOpera
376	tesseract-ocr Tesseract 缓冲区错误漏洞	CNNVD-2026-77705830	CVE-2026-88054	中危	https://github.com/tesseract-ocr/tesseract/security/advisories/GHSA-f6h7-cqr4-6fx4	tesseract-ocr
377	tesseract-ocr Tesseract 缓冲区错误漏洞	CNNVD-2026-10639408	CVE-2026-88050	中危	https://github.com/tesseract-ocr/tesseract/security/advisories/GHSA-7v9h-3q3m-w68g	tesseract-ocr
378	tile-ai tilelang 输入验证错误漏洞	CNNVD-2026-15987421	CVE-2026-87083	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。	tile-ai
379	vLLM 输入验证错误漏洞	CNNVD-2026-60735857	CVE-2026-93841	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	vLLM

					考网址以获取解决办法。	
380	vLLM 资源管理错误漏洞	CNNVD-2026-47239768	CVE-2026-92365	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。	vLLM
381	vLLM 资源管理错误漏洞	CNNVD-2026-20388469	CVE-2026-92220	中危	https://github.com/vllm-project/vllm/releases	vLLM
382	vLLM 资源管理错误漏洞	CNNVD-2026-14883569	CVE-2026-94625	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。	vLLM
383	vLLM 输入验证错误漏洞	CNNVD-2026-94083157	CVE-2026-93840	中危	https://github.com/vllm-project/vllm/commit/5b0e5b69ac1a3884a6479c9537789c95263cc804	vLLM
384	vLLM 资源管理错误漏洞	CNNVD-2026-34523622	CVE-2026-69147	中危	https://github.com/vllm-project/vllm/releases	vLLM
385	vLLM 资源管理错误漏洞	CNNVD-2026-62808107	CVE-2026-57173	中危	https://github.com/vllm-	vLLM

					project/vllm/releases	
386	vLLM 资源管理错误漏洞	CNNVD-2026-71060216	CVE-2026-90554	中危	https://github.com/vllm-project/vllm/security/advisories/GHSA-936p-m5pv-vvjf	vLLM
387	vLLM 资源管理错误漏洞	CNNVD-2026-90562600	CVE-2026-100649	中危	https://github.com/vllm-project/vllm/security/advisories/GHSA-j682-9xp5-rrf3	vLLM
388	vLLM 资源管理错误漏洞	CNNVD-2026-31171244	CVE-2026-100648	中危	https://github.com/vllm-project/vllm/security/advisories/GHSA-jcq2-4gch-5qhf	vLLM
389	vLLM 输入验证错误漏洞	CNNVD-2026-27415353	CVE-2026-100647	中危	https://github.com/vllm-project/vllm/security/advisories/GHSA-wpww-v874-ph2p	vLLM
390	WordPress AI Engine 授权问题漏洞	CNNVD-2026-30858374	CVE-2026-89141	中危	https://wordpress.org/plugins/ai-engine/	WordPress
391	WordPress AI Engine 授权问题漏洞	CNNVD-2026-98098746	CVE-2026-93623	中危	https://wordpress.org/plugins/ai-engine/	WordPress
392	Yao Engine Yao Agents 授权问题漏洞	CNNVD-2026-34622410	CVE-2026-91774	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	Yao Engine

					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。	

（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-2026-34619595	超危
2	CNNVD-2026-98830536	高危
3	CNNVD-2026-94820222	高危

1. OpenClaw 加密问题漏洞（CNNVD-2026-34619595）

OpenClaw 是一个开源的智能人工助理。

OpenClaw for iOS 2026.7.1 版本至 2026.8.11 之前版本存在加密问题漏洞，该漏洞源于在控制界面中未强制执行已保存的网关 TLS PIN 码，攻击者利用该漏洞可以获取操作员权限并泄露凭据。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://github.com/openclaw/openclaw/security/advisories/GHSA-jjpc-p3xf-8g7p

2. vLLM 资源管理错误漏洞（CNNVD-2026-98830536）

vLLM 是一个开源的适用于 LLM 的高吞吐量和内存高效推理和服务引擎。

vLLM 0.28.0 之前版本存在资源管理错误漏洞，该漏洞源于内存过度分配，攻击者利用该漏洞可以导致 API 服务器进程崩溃。

目前厂商已发布升级补丁以修复漏洞，参考链接：

https://github.com/vllm-project/vllm/security/advisories/GHSA-99f2-hwrc-gvq8

3. Ollama 服务端请求伪造漏洞（CNNVD-2026-94820222）

Ollama 是 Ollama 公司开源的一个可以在本地设备上运行、管理和自定义大语言模型的工具。

Ollama 0.30.0 版本至 0.33.2 版本存在服务端请求伪造漏洞，该漏洞源于在拉取 tensor-layer 模型时未能验证重定向目标，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://ollama.com/