

人工智能重要漏洞通报

（2026 年第七期）

根据国家信息安全漏洞库（CNNVD）统计，近期（2026 年 4 月 29 日至 2026 年 5 月 17 日）共采集重要人工智能漏洞 364 个，CNNVD 对这些漏洞进行了收录。本周人工智能类漏洞主要涵盖了 OpenClaw、Ollama、Langflow 等多个厂商（项目）。CNNVD 对其危害等级进行了评价，其中超危漏洞 30 个，高危漏洞 136 个，中危漏洞 198 个。

（一）人工智能漏洞增长数量情况

近期 CNNVD 采集人工智能漏洞 364 个。

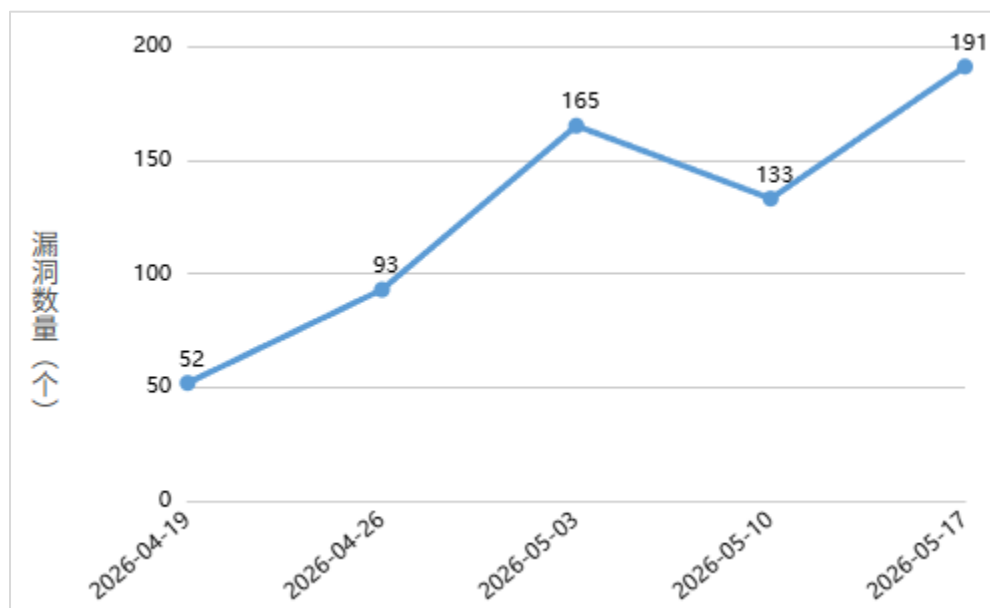


图 1 近五周漏洞新增数量统计图

（二）人工智能漏洞具体情况

近期共采集重要人工智能漏洞 364 个，包括 OpenClaw、Ollama、Langflow 等多个厂商（项目）的漏洞。其中超危漏洞 30 个，高危漏洞 136 个，中危漏洞 198 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	AstrBot 安全漏洞	CNNVD-202605-1814	CVE-2025-55449	超危	https://github.com/AstrBotDevs/AstrBot/releases	AstrBot
2	LiteLLM SQL 注入漏洞	CNNVD-202605-1853	CVE-2026-42208	超危	https://github.com/BerriAI/litellm/releases	Berri AI
3	Evolver 操作系统命令注入漏洞	CNNVD-202605-456	CVE-2026-42076	超危	https://github.com/EvoMap/evolver/releases	EvoMap
4	Gitroom Postiz 代码注入漏洞	CNNVD-202605-1482	CVE-2026-42298	超危	https://github.com/gitroomhq/postiz-app/releases	Gitroom
5	Jupyter Server 安全漏洞	CNNVD-202605-574	CVE-2026-40110	超危	https://github.com/jupyter-server/jupyter_server/releases	Jupyter
6	FastGPT 访问控制错误漏洞	CNNVD-202605-1480	CVE-2026-42302	超危	https://github.com/labring/FastGPT/releases	labring
7	Langflow 路径遍历漏洞	CNNVD-202605-2595	CVE-2026-42048	超危	https://github.com/langflow-ai/langflow/releases	Langflow
8	MindsDB 访问控制错误漏洞	CNNVD-202605-569	CVE-2026-7711	超危	https://github.com/mindsdb/mindsdb	MindsDB

					b/releases	
9	n8n 安全漏洞	CNNVD-202605-408	CVE-2026-42232	超危	https://github.com/n8n-io/n8n/releases	n8n
10	n8n 安全漏洞	CNNVD-202605-409	CVE-2026-42231	超危	https://github.com/n8n-io/n8n/releases	n8n
11	Ollama 缓冲区错误漏洞	CNNVD-202605-502	CVE-2026-7482	超危	https://github.com/ollama/ollama/releases	Ollama
12	Crabbox 代码注入漏洞	CNNVD-202605-3404	CVE-2026-8634	超危	https://github.com/openclaw/crabbox/releases/	openclaw
13	OpenClaw 安全漏洞	CNNVD-202605-679	CVE-2026-43566	超危	https://github.com/openclaw/openclaw/releases	OpenClaw
14	OpenClaw 数据伪造问题漏洞	CNNVD-202605-682	CVE-2026-43534	超危	https://github.com/openclaw/openclaw/releases	OpenClaw
15	GPT PILOT 安全漏洞	CNNVD-202605-2341	CVE-2026-31246	超危	https://github.com/Pythagora-io/gpt-pilot	Pythagora-io
16	Siemens Mendix Studio Pro 安全漏洞	CNNVD-202605-1266	CVE-2026-7891	超危	https://marketplace.mendix.com/index.html	Siemens
17	Siemens ROS# 安全漏洞	CNNVD-202605-2835	CVE-2026-41551	超危	https://cert-portal.siemens.com/productcert/html/ssa-357982.html	Siemens
18	Snorkel 安全漏洞	CNNVD-	CVE-2026-	超危	https://git	Snorkel

	洞	202605-2759	31223		hub.com/sno rkel- team/snorke l	
19	Snorkel 安全漏洞	CNNVD- 202605-2761	CVE-2026- 31224	超危	https://git hub.com/sno rkel- team/snorke l	Snorkel
20	Snorkel 安全漏洞	CNNVD- 202605-2762	CVE-2026- 31222	超危	https://git hub.com/sno rkel- team/snorke l	Snorkel
21	DeepChat 输入 验证错误漏洞	CNNVD- 202605-2054	CVE-2026- 43899	超危	https://git hub.com/Thi nkInAIXYZ/d eepchat/rel eases	ThinkInAI XYZ
22	DeepChat 跨站 脚本漏洞	CNNVD- 202605-2056	CVE-2026- 43900	超危	https://git hub.com/Thi nkInAIXYZ/d eepchat/rel eases	ThinkInAI XYZ
23	PraisonAI 命令 注入漏洞	CNNVD- 202605-1764	CVE-2026- 41497	超危	https://git hub.com/Mer vinPraison/ PraisonAI/r eleases	个人开发 者
24	sealed-env 信 息泄露漏洞	CNNVD- 202605-2799	CVE-2026- 45091	超危	https://git hub.com/dav idalmeidac/ sealed- env/release s	个人开发 者
25	open-notebook 安全漏洞	CNNVD- 202605-1384	CVE-2026- 33587	超危	https://git hub.com/lfn ovo/open- notebook/re leases	个人开发 者
26	open-notebook 安全漏洞	CNNVD- 202605-1385	CVE-2026- 28201	超危	https://git hub.com/lfn ovo/open- notebook/re leases	个人开发 者
27	open-notebook 安全漏洞	CNNVD- 202605-1388	CVE-2026- 33588	超危	https://git hub.com/lfn	个人开发 者

					ovo/open-notebook/releases	
28	phpMyFAQ SQL 注入漏洞	CNNVD-202605-3709	CVE-2026-46364	超危	https://www.phpmyfaq.de/	个人开发者
29	JunoClaw 信息泄露漏洞	CNNVD-202605-2716	CVE-2026-43992	超危	https://github.com/Dragonmonk111/junoclaw/releases	个人开发者
30	TinyZero 安全漏洞	CNNVD-202605-2755	CVE-2026-31226	超危	https://github.com/JiaYi-Pan/TinyZero	个人开发者
31	xhs-mcp 代码问题漏洞	CNNVD-202604-5573	CVE-2026-7417	高危	https://github.com/Algovate/xhs-mcp	Algovate
32	Amazon SageMaker Python SDK 安全漏洞	CNNVD-202605-3410	CVE-2026-8597	高危	https://github.com/aws/sagemaker-python-sdk/releases	Amazon
33	Amazon SageMaker Python SDK 安全漏洞	CNNVD-202605-3411	CVE-2026-8596	高危	https://github.com/aws/sagemaker-python-sdk/releases	Amazon
34	Claude Code 后置链接漏洞	CNNVD-202605-3120	CVE-2026-44470	高危	https://github.com/anthropics/claude-code/releases	Anthropic
35	Claude Code 安全漏洞	CNNVD-202605-3122	CVE-2026-44467	高危	https://github.com/anthropics/claude-code/releases	Anthropic
36	Argo Workflows 安全漏洞	CNNVD-202605-1927	CVE-2026-42296	高危	https://github.com/argoproj/argo-	Argo

					workflows/releases/	
37	AstrBot 安全漏洞	CNNVD-202605-228	CVE-2026-7579	高危	https://github.com/AstrBotDevs/AstrBot/releases	AstrBot
38	AgentFlow 代码注入漏洞	CNNVD-202604-5609	CVE-2026-7466	高危	https://github.com/berabuddies/agentflow	Bera Buddies
39	LiteLLM 命令注入漏洞	CNNVD-202605-1849	CVE-2026-42271	高危	https://github.com/BerriAI/litellm/releases	Berri AI
40	LiteLLM 安全漏洞	CNNVD-202605-1855	CVE-2026-42203	高危	https://github.com/BerriAI/litellm/releases	Berri AI
41	Budibase 安全漏洞	CNNVD-202605-1457	CVE-2026-42239	高危	https://github.com/Budibase/budibase/releases/	Budibase
42	daptin SQL 注入漏洞	CNNVD-202605-1348	CVE-2026-41422	高危	https://github.com/daptin/daptin/releases	Daptin
43	OpenHarness 操作系统命令注入漏洞	CNNVD-202604-5707	CVE-2026-7551	高危	https://github.com/HKUDS/OpenHarness/releases	Data Intelligence Lab@HKU
44	Evolver 路径遍历漏洞	CNNVD-202605-458	CVE-2026-42075	高危	https://github.com/EvoMap/evolver/releases	EvoMap
45	CosyVoice 安全漏洞	CNNVD-202605-2297	CVE-2026-31251	高危	https://github.com/FunAudioLLM/CosyVoice	FunAudioLLM
46	CosyVoice 安全漏洞	CNNVD-202605-2298	CVE-2026-31250	高危	https://github.com/FunAudioLLM/CosyVoice	FunAudioLLM
47	CosyVoice 安全漏洞	CNNVD-202605-2299	CVE-2026-31249	高危	https://github.com/Fun	FunAudioLLM

					AudioLLM/CosyVoice	
48	MCPoSimpleServer 路径遍历漏洞	CNNVD-202604-5580	CVE-2026-7404	高危	https://github.com/getsimpletool/mcpo-simple-server/	GetSimpleTool
49	GitHub Copilot CLI 安全漏洞	CNNVD-202605-3119	CVE-2026-45033	高危	https://github.com/github/copilot-cli/releases	GitHub
50	Gitroom Postiz 跨站脚本漏洞	CNNVD-202605-1464	CVE-2026-42556	高危	https://github.com/gitroomhq/postiz-app/releases	Gitroom
51	Heym 安全漏洞	CNNVD-202605-2426	CVE-2026-45226	高危	https://github.com/heyrun/heyrun/releases	heyrun
52	Heym 路径遍历漏洞	CNNVD-202605-2427	CVE-2026-45225	高危	https://github.com/heyrun/heyrun/releases	heyrun
53	Heym 安全漏洞	CNNVD-202605-2428	CVE-2026-45227	高危	https://github.com/heyrun/heyrun/releases	heyrun
54	diffusers 代码注入漏洞	CNNVD-202605-3468	CVE-2026-44827	高危	https://github.com/huggingface/diffusers/releases	Hugging Face
55	diffusers 代码注入漏洞	CNNVD-202605-3472	CVE-2026-44513	高危	https://github.com/huggingface/diffusers/releases	Hugging Face
56	IBM Langflow Desktop 代码注入漏洞	CNNVD-202604-5709	CVE-2026-6543	高危	https://www.ibm.com/support/pages/node/7271092	IBM

57	IBM Turbonomic prometurbo agent 安全漏洞	CNNVD-202604-5712	CVE-2026-6389	高危	https://www.ibm.com/support/pages/node/7270720	IBM
58	IBM Langflow Desktop 安全漏洞	CNNVD-202604-5728	CVE-2026-4503	高危	https://www.ibm.com/support/pages/node/7271099	IBM
59	PPTAgent 安全漏洞	CNNVD-202605-453	CVE-2026-42079	高危	https://github.com/icip-cas/PPTAgent/releases	ICIP-CAS
60	Inkeep Agents 授权问题漏洞	CNNVD-202605-2179	CVE-2026-8321	高危	https://inkeep.com/	Inkeep
61	Intel Vision 访问控制错误漏洞	CNNVD-202605-2725	CVE-2026-20887	高危	https://intel.com/content/www/us/en/security-center/advisory/intel-sa-01457.html	Intel
62	Intel AI Playground 代码问题漏洞	CNNVD-202605-2738	CVE-2025-36515	高危	https://intel.com/content/www/us/en/security-center/advisory/intel-sa-01438.html	Intel
63	Jupyter Server 代码问题漏洞	CNNVD-202605-573	CVE-2026-40934	高危	https://github.com/jupyter-server/jupyter_server/releases	Jupyter
64	FastGPT 代码问题漏洞	CNNVD-202605-1475	CVE-2026-42345	高危	https://github.com/labring/FastGPT/releases	labring
65	Pytorch-Lightning 安全	CNNVD-202605-2760	CVE-2026-31221	高危	https://github.com/LightningAI	Lightning AI

	漏洞				htning-AI/pytorch-lightning/releases	
66	Microsoft Azure AI Foundry M365 published agents 访问控制错误漏洞	CNNVD-202605-1272	CVE-2026-35435	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35435	Microsoft
67	Microsoft Copilot Chat 命令注入漏洞	CNNVD-202605-1277	CVE-2026-33111	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33111	Microsoft
68	Microsoft 365 Copilot BizChat 注入漏洞	CNNVD-202605-1280	CVE-2026-26164	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26164	Microsoft
69	Microsoft 365 Copilot Business Chat 安全漏洞	CNNVD-202605-1281	CVE-2026-26129	高危	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26129	Microsoft
70	APM - Agent Package Manager 后置链接漏洞	CNNVD-202605-3740	CVE-2026-45539	高危	https://github.com/microsoft/apm/releases	Microsoft
71	APM - Agent Package Manager 路径遍历漏洞	CNNVD-202605-3748	CVE-2026-44641	高危	https://github.com/microsoft/apm/releases	Microsoft
72	MindsDB 输入验证错误漏洞	CNNVD-202605-572	CVE-2026-7712	高危	https://github.com/mindsdb/mindsd	MindsDB

					b/releases	
73	MLflow 代码问题漏洞	CNNVD-202605-2285	CVE-2026-2393	高危	https://github.com/mlflow/mlflow/releases	MLflow
74	MLflow 安全漏洞	CNNVD-202605-3827	CVE-2026-2652	高危	https://github.com/mlflow/mlflow/releases	MLflow
75	MLflow 路径遍历漏洞	CNNVD-202605-2201	CVE-2026-2614	高危	https://github.com/mlflow/mlflow/releases	MLflow
76	RMCP 访问控制错误漏洞	CNNVD-202605-3514	CVE-2026-42559	高危	https://github.com/modelcontextprotocol/rust-sdk/releases	Model Context Protocol
77	n8n SQL 注入漏洞	CNNVD-202605-401	CVE-2026-42237	高危	https://github.com/n8n-io/n8n/releases	n8n
78	n8n 跨站脚本漏洞	CNNVD-202605-404	CVE-2026-42235	高危	https://github.com/n8n-io/n8n/releases	n8n
79	n8n 安全漏洞	CNNVD-202605-405	CVE-2026-42236	高危	https://github.com/n8n-io/n8n/releases	n8n
80	n8n SQL 注入漏洞	CNNVD-202605-407	CVE-2026-42233	高危	https://github.com/n8n-io/n8n/releases	n8n
81	n8n 安全漏洞	CNNVD-202605-413	CVE-2026-42227	高危	https://github.com/n8n-io/n8n/releases	n8n
82	n8n 安全漏洞	CNNVD-202605-414	CVE-2026-42226	高危	https://github.com/n8n-io/n8n/releases	n8n

					- io/n8n/releases	
83	goclaw 安全漏洞	CNNVD-202604-5704	CVE-2026-7505	高危	https://github.com/nextlevelbuilder/goclaw/releases	Next Level Builder
84	NextChat 安全漏洞	CNNVD-202605-272	CVE-2026-7644	高危	https://github.com/ChatGPTNextWeb/NextChat/releases	NextChat
85	Nocobase SQL 注入漏洞	CNNVD-202605-1407	CVE-2026-41641	高危	https://github.com/nocobase/nocobase/releases	NocoBase
86	Nocobase SQL 注入漏洞	CNNVD-202605-1437	CVE-2026-41640	高危	https://github.com/nocobase/nocobase/releases	NocoBase
87	Ollama 路径遍历漏洞	CNNVD-202604-5679	CVE-2026-42249	高危	https://ollama.com/	Ollama
88	Ollama 安全漏洞	CNNVD-202604-5680	CVE-2026-42248	高危	https://ollama.com/	Ollama
89	Open WebUI 跨站脚本漏洞	CNNVD-202605-3643	CVE-2026-45665	高危	https://github.com/open-webui/open-webui/releases	Open WebUI
90	Open WebUI 安全漏洞	CNNVD-202605-3647	CVE-2026-45350	高危	https://github.com/open-webui/open-webui/releases	Open WebUI
91	Open WebUI 跨站脚本漏洞	CNNVD-202605-3654	CVE-2026-45315	高危	https://github.com/open-webui/open-webui/releases	Open WebUI
92	Open WebUI 代码问题漏洞	CNNVD-202605-3655	CVE-2026-45338	高危	https://github.com/open-webui/open-webui	Open WebUI

					n- webui/open- webui/relea ses	
93	Open WebUI 跨 站脚本漏洞	CNNVD- 202605-3657	CVE-2026- 45303	高危	https://git hub.com/ope n- webui/open- webui/relea ses	Open WebUI
94	Open WebUI 访 问控制错误漏洞	CNNVD- 202605-3658	CVE-2026- 45301	高危	https://git hub.com/ope n- webui/open- webui/relea ses	Open WebUI
95	Open WebUI 路 径遍历漏洞	CNNVD- 202605-3662	CVE-2026- 44566	高危	https://git hub.com/ope n- webui/open- webui/relea ses	Open WebUI
96	Open WebUI 安 全漏洞	CNNVD- 202605-3668	CVE-2026- 45672	高危	https://git hub.com/ope n- webui/open- webui/relea ses	Open WebUI
97	Open WebUI 安 全漏洞	CNNVD- 202605-3669	CVE-2026- 45402	高危	https://git hub.com/ope n- webui/open- webui/relea ses	Open WebUI
98	Open WebUI 代 码问题漏洞	CNNVD- 202605-3670	CVE-2026- 45400	高危	https://git hub.com/ope n- webui/open- webui/relea ses	Open WebUI
99	Open WebUI 安 全漏洞	CNNVD- 202605-3678	CVE-2026- 45675	高危	https://git hub.com/ope n- webui/open- webui/relea ses	Open WebUI
100	Open WebUI 跨	CNNVD-	CVE-2026-	高危	https://git	Open

	站脚本漏洞	202605-3680	44721		hub.com/open-webui/releases	WebUI
101	Open WebUI 安全漏洞	CNNVD-202605-3681	CVE-2026-45399	高危	https://github.com/open-webui/releases	Open WebUI
102	Open WebUI 安全漏洞	CNNVD-202605-3682	CVE-2026-45671	高危	https://github.com/open-webui/releases	Open WebUI
103	Open WebUI 安全漏洞	CNNVD-202605-3684	CVE-2026-45349	高危	https://github.com/open-webui/releases	Open WebUI
104	Open WebUI 代码问题漏洞	CNNVD-202605-3685	CVE-2026-45331	高危	https://github.com/open-webui/releases	Open WebUI
105	Open WebUI 安全漏洞	CNNVD-202605-3695	CVE-2026-44555	高危	https://github.com/open-webui/releases	Open WebUI
106	Open WebUI 安全漏洞	CNNVD-202605-3696	CVE-2026-44554	高危	https://github.com/open-webui/releases	Open WebUI
107	Open WebUI 代码问题漏洞	CNNVD-202605-3697	CVE-2026-44553	高危	https://github.com/open-webui/releases	Open WebUI

108	Open WebUI 安全漏洞	CNNVD-202605-3698	CVE-2026-44552	高危	https://github.com/open-webui/open-webui/releases	Open WebUI
109	Open WebUI 访问控制错误漏洞	CNNVD-202605-3700	CVE-2026-44556	高危	https://github.com/open-webui/open-webui/releases	Open WebUI
110	Crabbox 安全漏洞	CNNVD-202605-3408	CVE-2026-8629	高危	https://github.com/openclaw/crabbox/releases/	openclaw
111	Crabbox 授权问题漏洞	CNNVD-202605-3429	CVE-2026-8621	高危	https://github.com/openclaw/crabbox/releases/	openclaw
112	OpenClaw 安全漏洞	CNNVD-202605-671	CVE-2026-43573	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
113	Crabbox 安全漏洞	CNNVD-202605-2204	CVE-2026-45223	高危	https://github.com/openclaw/crabbox/releases	openclaw
114	OpenClaw 安全漏洞	CNNVD-202605-674	CVE-2026-43571	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
115	Crabbox 路径遍历漏洞	CNNVD-202605-2208	CVE-2026-45224	高危	https://github.com/openclaw/crabbox/releases	openclaw
116	OpenClaw 安全漏洞	CNNVD-202605-676	CVE-2026-43569	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
117	OpenClaw 授权问题漏洞	CNNVD-202605-2213	CVE-2026-8305	高危	https://github.com/openclaw/openclaw/releases	OpenClaw

					nclaw/openc law/release s	
118	OpenClaw 安全 漏洞	CNNVD- 202605-681	CVE-2026- 43533	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
119	OpenClaw 安全 漏洞	CNNVD- 202605-683	CVE-2026- 43532	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
120	OpenClaw 安全 漏洞	CNNVD- 202605-684	CVE-2026- 43531	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
121	OpenClaw 安全 漏洞	CNNVD- 202605-686	CVE-2026- 43530	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
122	OpenClaw 代码 问题漏洞	CNNVD- 202605-688	CVE-2026- 43527	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
123	OpenClaw 安全 漏洞	CNNVD- 202605-689	CVE-2026- 42439	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
124	OpenClaw 安全 漏洞	CNNVD- 202605-2222	CVE-2026- 45006	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
125	OpenClaw 代码 问题漏洞	CNNVD- 202605-690	CVE-2026- 43526	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
126	OpenClaw 安全 漏洞	CNNVD- 202605-691	CVE-2026- 42438	高危	https://github.com/openclaw/openclaw/releases	OpenClaw

					s	
127	OpenClaw 代码 问题漏洞	CNNVD- 202605-2224	CVE-2026- 45004	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
128	OpenClaw 安全 漏洞	CNNVD- 202605-692	CVE-2026- 42437	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
129	OpenClaw 安全 漏洞	CNNVD- 202605-693	CVE-2026- 42436	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
130	OpenClaw 安全 漏洞	CNNVD- 202605-2226	CVE-2026- 45001	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
131	OpenClaw 安全 漏洞	CNNVD- 202605-694	CVE-2026- 42435	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
132	OpenClaw 安全 漏洞	CNNVD- 202605-695	CVE-2026- 42434	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
133	OpenClaw 安全 漏洞	CNNVD- 202605-2234	CVE-2026- 44995	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
134	Oracle MCP Server Helper Tool SQL 注入 漏洞	CNNVD- 202605-728	CVE-2026- 35228	高危	https://www.oracle.com/security-alerts/all-oracle-cves-outside-other-oracle-public-documents.h	Oracle

					tml	
135	New API 数据伪造问题漏洞	CNNVD-202605-1488	CVE-2026-41432	高危	https://github.com/QuantumNous/new-api/releases/	QuantumNous
136	OpenLearnX 操作系统命令注入漏洞	CNNVD-202605-1856	CVE-2026-41900	高危	https://github.com/th30d4y/OpenLearnX/releases/	th30d4y
137	Vercel AI SDK 代码问题漏洞	CNNVD-202605-3902	CVE-2026-8768	高危	https://github.com/vercel/ai/releases	Vercel
138	MCP Server Semgrep 命令注入漏洞	CNNVD-202604-5870	CVE-2026-7446	高危	https://github.com/VetCoders/mcp-server-semgrep/releases	VetCoders
139	VMware Spring AI 安全漏洞	CNNVD-202605-2820	CVE-2026-41713	高危	https://spring.io/projects/spring-ai	VMware
140	VMware Spring AI 安全漏洞	CNNVD-202605-2821	CVE-2026-41712	高危	https://spring.io/projects/spring-ai	VMware
141	Filesystem MCP Server 路径遍历漏洞	CNNVD-202604-5586	CVE-2026-7400	高危	https://github.com/geekgod382/filesystem-mcp-server/tags	个人开发者
142	PraisonAI SQL 注入漏洞	CNNVD-202605-1765	CVE-2026-41496	高危	https://github.com/MervinPraison/PraisonAI/releases	个人开发者
143	Open-WebSearch 代码问题漏洞	CNNVD-202605-2790	CVE-2026-42260	高危	https://github.com/Aasee/open-webSearch/releases	个人开发者
144	NagaAgent 路径	CNNVD-	CVE-2026-	高危	https://git	个人开发

	遍历漏洞	202605-750	7784		hub.com/RTGS2017/NagaAgent/	者
145	BioinfoMCP 路径遍历漏洞	CNNVD-202604-5613	CVE-2026-7398	高危	https://github.com/florensiawidja/BioinfoMCP	个人开发者
146	command-executor MCP Server 命令注入漏洞	CNNVD-202605-006	CVE-2026-7593	高危	https://github.com/Sunwood-ai-labs/command-executor-mcp-server/	个人开发者
147	n8n-MCP 代码问题漏洞	CNNVD-202605-1285	CVE-2026-42449	高危	https://n8n.io/	个人开发者
148	changedetection.io 安全漏洞	CNNVD-202605-2577	CVE-2026-43891	高危	https://github.com/dgtlmoon/changedetection.io/releases	个人开发者
149	Mail MCP Bridge 路径遍历漏洞	CNNVD-202604-5637	CVE-2026-7386	高危	https://github.com/fatbobman/mail-mcp-bridge/releases/tag/1.3.4	个人开发者
150	MCP Research Assistant 路径遍历漏洞	CNNVD-202604-5653	CVE-2026-7384	高危	https://github.com/ezequiroga/mcp-bases/	个人开发者
151	PromptHub 输入验证错误漏洞	CNNVD-202605-1852	CVE-2026-42261	高危	https://github.com/legeling/PromptHub/releases/	个人开发者
152	phpMyFAQ 跨站脚本漏洞	CNNVD-202605-3707	CVE-2026-46367	高危	https://www.phpmyfaq.de/	个人开发者
153	phpMyFAQ 安全漏洞	CNNVD-202605-3708	CVE-2026-46366	高危	https://www.phpmyfaq.de/	个人开发者
154	phpMyFAQ SQL 注入漏洞	CNNVD-202605-3716	CVE-2026-46359	高危	https://www.phpmyfaq.de/	个人开发者
155	PraisonAI 路径	CNNVD-	CVE-2026-	高危	https://git	个人开发

	遍历漏洞	202605-1682	44340		hub.com/MervinPraison/PraisonAI/releases	者
156	PraisonAI 安全漏洞	CNNVD-202605-1684	CVE-2026-44339	高危	https://github.com/MervinPraison/PraisonAI/releases	个人开发者
157	PraisonAI 访问控制错误漏洞	CNNVD-202605-1685	CVE-2026-44338	高危	https://github.com/MervinPraison/PraisonAI/releases	个人开发者
158	PraisonAI 代码问题漏洞	CNNVD-202605-1687	CVE-2026-44335	高危	https://github.com/MervinPraison/PraisonAI/releases	个人开发者
159	PraisonAI 输入验证错误漏洞	CNNVD-202605-1688	CVE-2026-44336	高危	https://github.com/MervinPraison/PraisonAI/releases	个人开发者
160	PraisonAI 代码注入漏洞	CNNVD-202605-1689	CVE-2026-44334	高危	https://github.com/MervinPraison/PraisonAI/releases	个人开发者
161	JunoClaw 代码问题漏洞	CNNVD-202605-2715	CVE-2026-43993	高危	https://github.com/Dragonmonk111/junoclaw/releases	个人开发者
162	JunoClaw 命令注入漏洞	CNNVD-202605-2719	CVE-2026-43990	高危	https://github.com/Dragonmonk111/junoclaw/releases	个人开发者
163	JunoClaw 输入验证错误漏洞	CNNVD-202605-2721	CVE-2026-43989	高危	https://github.com/Dragonmonk111/junoclaw/releases	个人开发者
164	Network-AI 访问控制错误漏洞	CNNVD-202605-2256	CVE-2026-42856	高危	https://github.com/Jovancoding/Ne	个人开发者

					work- AI/releases	
165	Python Notebook MCP 路径遍历漏洞	CNNVD- 202605-724	CVE-2026- 7810	高危	https://github.com/UsamaK98/python-notebook-mcp/	个人开发者
166	Xcode MCP Server 命令注入漏洞	CNNVD- 202604-5577	CVE-2026- 7416	高危	https://github.com/PolarVista/Xcode-mcp-server	个人开发者
167	Aegra 授权问题 漏洞	CNNVD- 202605-3490	CVE-2026- 44504	中危	https://github.com/aegra/aegra/releases	Aegra
168	agents 资源管理 错误漏洞	CNNVD- 202605-2180	CVE-2026- 8319	中危	https://github.com/aiwaves-cn/agents/	AIWaves
169	Claude Code 输入 验证错误漏洞	CNNVD- 202605-578	CVE-2026- 40068	中危	https://github.com/anthropics/claude-code/releases	Anthropic
170	Claude SDK for TypeScript 安全漏洞	CNNVD- 202605-418	CVE-2026- 41686	中危	https://github.com/anthropics/anthropic-sdk-typescript/releases	Anthropic
171	Apache OpenNLP 安全漏洞	CNNVD- 202605-445	CVE-2026- 42440	中危	https://lists.apache.org/thread/s8xlkxlgqbxfsq48py5h6jphjvgqpljo	Apache
172	Apache OpenNLP 安全漏洞	CNNVD- 202605-459	CVE-2026- 42027	中危	https://lists.apache.org/thread/tlo4powjfc0w2w2yyl1o5tc7qlgcb2y	Apache
173	Apache OpenNLP 代码问题漏洞	CNNVD- 202605-461	CVE-2026- 40682	中危	https://lists.apache.org/thread/r	Apache

					6jpt0qr9nj6 7gqhppqg7jx f8vsbo0w6	
174	DocsGPT 命令注入漏洞	CNNVD- 202604-5625	CVE-2026- 26015	中危	https://github.com/arc53/DocsGPT/releases/	Arc53
175	Argo Workflows 安全漏洞	CNNVD- 202605-1926	CVE-2026- 42297	中危	https://github.com/argoproj/argo-workflows/releases/	Argo
176	Argo Workflows 安全漏洞	CNNVD- 202605-1928	CVE-2026- 42295	中危	https://github.com/argoproj/argo-workflows/releases/	Argo
177	Argo Workflows 安全漏洞	CNNVD- 202605-1929	CVE-2026- 42294	中危	https://github.com/argoproj/argo-workflows/releases/	Argo
178	Argo Workflows 代码问题漏洞	CNNVD- 202605-1930	CVE-2026- 42183	中危	https://github.com/argoproj/argo-workflows/releases/	Argo
179	AstrBot 路径遍历漏洞	CNNVD- 202605-3921	CVE-2026- 8754	中危	https://github.com/AstrBotDevs/AstrBot/releases	AstrBot
180	genie 安全漏洞	CNNVD- 202605-2276	CVE-2026- 30635	中危	https://github.com/automagik-dev/genie/releases	automagik
181	AgentFlow 访问控制错误漏洞	CNNVD- 202604-5610	CVE-2026- 7439	中危	https://github.com/berabuddies/agentflow	Bera Buddies
182	LangChain-Chatcat 授权问题漏洞	CNNVD- 202605-625	CVE-2026- 7844	中危	https://github.com/chatcat-space/LangChain-Chatcat/	Chatcat-Space

183	Archon 安全漏洞	CNNVD-202605-3525	CVE-2025-69443	中危	https://github.com/colcam00/Archon/releases	CMS
184	FlashAttention 安全漏洞	CNNVD-202605-2292	CVE-2026-31254	中危	https://github.com/Dao-AILab/flash-attention/releases	Dao AI Lab
185	FlashAttention 安全漏洞	CNNVD-202605-2294	CVE-2026-31253	中危	https://github.com/Dao-AILab/flash-attention/releases	Dao AI Lab
186	daptin SQL 注入漏洞	CNNVD-202605-1342	CVE-2026-44349	中危	https://github.com/daptin/daptin/releases	Daptin
187	SQLBot SQL 注入漏洞	CNNVD-202605-611	CVE-2026-33324	中危	https://community.fit2cloud.com/#/products/sqlbot/downloads	DataEase
188	Docling 安全漏洞	CNNVD-202605-2305	CVE-2026-31248	中危	https://github.com/docling-project/docling/releases	Docling Project
189	Docling 安全漏洞	CNNVD-202605-2336	CVE-2026-31247	中危	https://github.com/docling-project/docling/releases	Docling Project
190	Evolver 安全漏洞	CNNVD-202605-454	CVE-2026-42077	中危	https://github.com/EvoMap/evolver/releases	EvoMap
191	Flowise 代码问题漏洞	CNNVD-202605-2244	CVE-2026-43995	中危	https://flowiseai.com/	FlowiseAI
192	FluentCMS 跨站	CNNVD-	CVE-2025-	中危	https://fluentcms.com/	FluentCMS

	脚本漏洞	202605-2792	70842		entcms.com/	
193	CosyVoice 安全漏洞	CNNVD-202605-2296	CVE-2026-31252	中危	https://github.com/FunAudioLLM/CosyVoice	FunAudioLLM
194	CosyVoice 安全漏洞	CNNVD-202605-2696	CVE-2026-31232	中危	https://github.com/FunAudioLLM/CosyVoice/tags	FunAudioLLM
195	Gel MCP server 路径遍历漏洞	CNNVD-202604-5579	CVE-2026-7403	中危	https://github.com/geldata/gel-mcp/	Gel
196	Gitroom Postiz 代码问题漏洞	CNNVD-202605-1474	CVE-2026-42346	中危	https://github.com/gitroomhq/postiz-app/releases	Gitroom
197	Guardrails 安全漏洞	CNNVD-202605-2695	CVE-2026-31233	中危	https://github.com/guardrails-ai/guardrails/releases	Guardrails AI
198	HCL AION 安全漏洞	CNNVD-202605-3483	CVE-2025-62313	中危	https://support.hcl-software.com/csm?id=kb_article&sysparm_article=KB0130636	HCL
199	HCL AION 安全漏洞	CNNVD-202605-3485	CVE-2025-62311	中危	https://support.hcl-software.com/csm?id=kb_article&sysparm_article=KB0130636	HCL
200	HCL AION 安全漏洞	CNNVD-202605-3486	CVE-2025-62310	中危	https://support.hcl-software.com/csm?id=kb_article&sysparm_article=KB0130636	HCL

					le=KB0130636	
201	HCL AION 安全漏洞	CNNVD-202605-3488	CVE-2025-62308	中危	https://support.hcl-software.com/csm?id=kb_article&sysparm_article=KB0130636	HCL
202	HCL AION 安全漏洞	CNNVD-202605-3489	CVE-2025-62305	中危	https://support.hcl-software.com/csm?id=kb_article&sysparm_article=KB0130636	HCL
203	Horovod 安全漏洞	CNNVD-202605-2694	CVE-2026-31234	中危	https://github.com/horovod/horovod/releases	Horovod
204	IBM Langflow 安全漏洞	CNNVD-202604-5711	CVE-2026-6542	中危	https://www.ibm.com/support/pages/node/7270886	IBM
205	IBM Langflow Desktop 路径遍历漏洞	CNNVD-202604-5717	CVE-2026-3345	中危	https://www.ibm.com/support/pages/node/7271094	IBM
206	IBM Watsonx.data 安全漏洞	CNNVD-202604-5718	CVE-2025-36180	中危	https://www.ibm.com/support/pages/node/7270593	IBM
207	IBM watsonx.data intelligence 安全漏洞	CNNVD-202604-5719	CVE-2025-36335	中危	https://www.ibm.com/support/pages/node/7270923	IBM
208	IBM Langflow Desktop 路径遍历漏洞	CNNVD-202604-5726	CVE-2026-4502	中危	https://www.ibm.com/support/pages/node/7271097	IBM

209	IBM Langflow Desktop SQL 注入漏洞	CNNVD-202604-5733	CVE-2026-3346	中危	https://www.ibm.com/support/pages/node/7271095	IBM
210	IBM Langflow Desktop 代码问题漏洞	CNNVD-202604-5736	CVE-2026-3340	中危	https://www.ibm.com/support/pages/node/7271096	IBM
211	PPTAgent 路径遍历漏洞	CNNVD-202605-455	CVE-2026-42080	中危	https://github.com/icip-cas/PPTAgent/releases	ICIP-CAS
212	PPTAgent 路径遍历漏洞	CNNVD-202605-457	CVE-2026-42078	中危	https://github.com/icip-cas/PPTAgent/releases	ICIP-CAS
213	Jupyter Server 路径遍历漏洞	CNNVD-202605-589	CVE-2026-35397	中危	https://github.com/jupyter-server/jupyter_server/releases	Jupyter
214	Jupyter Server 输入验证错误漏洞	CNNVD-202605-652	CVE-2025-61669	中危	https://github.com/jupyter-server/jupyter_server/releases	Jupyter
215	Kilo Code 信息泄露漏洞	CNNVD-202605-3903	CVE-2026-8766	中危	https://github.com/KiloOrg/kilocode/releases	Kilo Code
216	Kilo Code 路径遍历漏洞	CNNVD-202605-3904	CVE-2026-8765	中危	https://github.com/KiloOrg/kilocode/releases	Kilo Code
217	FastGPT 代码问题漏洞	CNNVD-202605-1463	CVE-2026-44286	中危	https://github.com/labring/FastGPT/releases	labring
218	FastGPT 代码问	CNNVD-	CVE-2026-	中危	https://git	labring

	题漏洞	202605-1465	44284		hub.com/labring/FastGPT/releases	
219	FastGPT 资源管理错误漏洞	CNNVD-202605-1477	CVE-2026-42343	中危	https://github.com/labring/FastGPT/releases	labring
220	FastGPT 安全漏洞	CNNVD-202605-1479	CVE-2026-42344	中危	https://github.com/labring/FastGPT/releases	labring
221	Langflow 注入漏洞	CNNVD-202605-347	CVE-2026-7700	中危	https://github.com/langflow-ai/langflow/releases	Langflow
222	Langflow 注入漏洞	CNNVD-202605-360	CVE-2026-7687	中危	https://github.com/langflow-ai/langflow/releases	Langflow
223	langfuse 访问控制错误漏洞	CNNVD-202605-1677	CVE-2026-41487	中危	https://github.com/langfuse/langfuse/releases	Langfuse
224	dify 安全漏洞	CNNVD-202605-577	CVE-2026-41950	中危	https://github.com/langgenius/dify/releases	LangGenius
225	dify 跨站脚本漏洞	CNNVD-202605-425	CVE-2026-42138	中危	https://github.com/langgenius/dify/releases	LangGenius
226	PyTorch Lightning 安全漏洞	CNNVD-202605-3506	CVE-2026-44484	中危	https://github.com/Lightning-AI/pytorch-lightning/releases	Lightning AI
227	LobeHub 跨站脚本漏洞	CNNVD-202605-2594	CVE-2026-42045	中危	https://github.com/lobehub/lobehub/releases	LobeHub
228	ludwig 安全漏洞	CNNVD-202605-2688	CVE-2026-31238	中危	https://ludwig.ai/latest/	Ludwig

229	ludwig 安全漏洞	CNNVD-202605-2690	CVE-2026-31237	中危	https://ludwig.ai/latest/	Ludwig
230	mem0 输入验证错误漏洞	CNNVD-202605-003	CVE-2026-7597	中危	https://mem0.ai/	Mem0
231	mem0 安全漏洞	CNNVD-202605-2681	CVE-2026-31245	中危	https://github.com/mem0ai/mem0/releases	Mem0
232	mem0 安全漏洞	CNNVD-202605-2682	CVE-2026-31244	中危	https://github.com/mem0ai/mem0/releases	Mem0
233	mem0 安全漏洞	CNNVD-202605-2685	CVE-2026-31243	中危	https://github.com/mem0ai/mem0/releases	Mem0
234	mem0 安全漏洞	CNNVD-202605-2686	CVE-2026-31242	中危	https://github.com/mem0ai/mem0/releases	Mem0
235	mem0 安全漏洞	CNNVD-202605-2687	CVE-2026-31241	中危	https://github.com/mem0ai/mem0/releases	Mem0
236	mem0 安全漏洞	CNNVD-202605-2691	CVE-2026-31240	中危	https://github.com/mem0ai/mem0/releases	Mem0
237	nnU-Net 安全漏洞	CNNVD-202605-2460	CVE-2026-44246	中危	https://github.com/MIC-DKFZ/nnUNet/releases	MIC-DKFZ
238	APM - Agent Package Manager 路径遍历漏洞	CNNVD-202605-3739	CVE-2026-46383	中危	https://github.com/microsoft/apm/releases	Microsoft
239	AnythingLLM 信息泄露漏洞	CNNVD-202605-1467	CVE-2026-42456	中危	https://github.com/Mintplex-Labs/anything-llm/releases	Mintplex
240	MCP Registry 跨站脚本漏洞	CNNVD-202605-3397	CVE-2026-44429	中危	https://github.com/mod	Model Context

					elcontextpr otocol/regi stry/releas es	Protocol
241	MCP Registry 安全漏洞	CNNVD- 202605-3398	CVE-2026- 45781	中危	https://git hub.com/mod elcontextpr otocol/regi stry/releas es	Model Context Protocol
242	MCP Registry 代码问题漏洞	CNNVD- 202605-3403	CVE-2026- 44430	中危	https://git hub.com/mod elcontextpr otocol/regi stry/releas es	Model Context Protocol
243	MCP Registry 输入验证错误漏 洞	CNNVD- 202605-3405	CVE-2026- 44427	中危	https://git hub.com/mod elcontextpr otocol/regi stry/releas es	Model Context Protocol
244	MCP Registry 代码问题漏洞	CNNVD- 202605-3406	CVE-2026- 44428	中危	https://git hub.com/mod elcontextpr otocol/regi stry/releas es	Model Context Protocol
245	Nexent 安全漏 洞	CNNVD- 202605-2766	CVE-2026- 31216	中危	https://git hub.com/Mod elEngine- Group/nexen t/releases	ModelEngi ne-Group
246	Nexent 安全漏 洞	CNNVD- 202605-2771	CVE-2026- 31215	中危	https://git hub.com/Mod elEngine- Group/nexen t/releases	ModelEngi ne-Group
247	n8n 代码注入漏 洞	CNNVD- 202605-406	CVE-2026- 42234	中危	https://git hub.com/n8n - io/n8n/rele ases	n8n
248	n8n SQL 注入漏 洞	CNNVD- 202605-410	CVE-2026- 42229	中危	https://git hub.com/n8n - io/n8n/rele	n8n

					ases	
249	n8n 安全漏洞	CNNVD-202605-411	CVE-2026-42228	中危	https://github.com/n8n-io/n8n/releases	n8n
250	n8n 输入验证错误漏洞	CNNVD-202605-412	CVE-2026-42230	中危	https://github.com/n8n-io/n8n/releases	n8n
251	OptiMate 安全漏洞	CNNVD-202605-2764	CVE-2026-31218	中危	https://github.com/nebuly-ai/optimate	Nebuly
252	OptiMate 安全漏洞	CNNVD-202605-2765	CVE-2026-31217	中危	https://github.com/nebuly-ai/optimate	Nebuly
253	OptiMate 安全漏洞	CNNVD-202605-2773	CVE-2026-31219	中危	https://github.com/nebuly-ai/optimate	Nebuly
254	UI UX Pro Max 跨站脚本漏洞	CNNVD-202605-004	CVE-2026-7596	中危	https://www.uupm.cc/	Next Level Builder
255	UI UX Pro Max 注入漏洞	CNNVD-202605-005	CVE-2026-7595	中危	https://www.uupm.cc/	Next Level Builder
256	NextChat 访问控制错误漏洞	CNNVD-202605-273	CVE-2026-7643	中危	https://github.com/ChatGPTNextWeb/NextChat/releases	NextChat
257	Hermes Agent 后置链接漏洞	CNNVD-202604-5615	CVE-2026-7397	中危	https://github.com/NousResearch/hermes-agent/releases	Nous Research
258	Hermes Agent 路径遍历漏洞	CNNVD-202604-5620	CVE-2026-7396	中危	https://github.com/NousResearch/hermes-agent/releases	Nous Research
259	oinone-pamirs	CNNVD-	CVE-2026-	中危	https://oin	Oinone

	命令注入漏洞	202605-3774	39054		one.ai/zh	
260	oinone-pamirs 代码问题漏洞	CNNVD-202605-3775	CVE-2026-39053	中危	https://oinone.ai/zh	Oinone
261	oinone-pamirs 代码注入漏洞	CNNVD-202605-3778	CVE-2026-39052	中危	https://oinone.ai/zh	Oinone
262	Onyx 安全漏洞	CNNVD-202605-1826	CVE-2026-42277	中危	https://github.com/onyx-dot-app/onyx/releases	Onyx
263	Onyx 安全漏洞	CNNVD-202605-1827	CVE-2026-42276	中危	https://github.com/onyx-dot-app/onyx/releases	Onyx
264	Open WebUI 授权问题漏洞	CNNVD-202605-3645	CVE-2026-45365	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
265	Open WebUI 信息泄露漏洞	CNNVD-202605-3646	CVE-2026-45351	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
266	Open WebUI 安全漏洞	CNNVD-202605-3656	CVE-2026-45314	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
267	Open WebUI 跨站脚本漏洞	CNNVD-202605-3659	CVE-2026-45299	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
268	Open WebUI 安全漏洞	CNNVD-202605-3660	CVE-2026-44571	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
269	Open WebUI 安全漏洞	CNNVD-202605-3675	CVE-2026-45386	中危	https://github.com/open-webui/open-webui/releases	Open WebUI

					n- webui/open- webui/relea ses	
270	Open WebUI 信 息泄露漏洞	CNNVD- 202605-3676	CVE-2026- 45387	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
271	Open WebUI 安 全漏洞	CNNVD- 202605-3679	CVE-2026- 45396	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
272	Open WebUI 安 全漏洞	CNNVD- 202605-3686	CVE-2026- 44564	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
273	Open WebUI 跨 站脚本漏洞	CNNVD- 202605-3688	CVE-2026- 44568	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
274	Open WebUI 安 全漏洞	CNNVD- 202605-3689	CVE-2026- 44561	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
275	Open WebUI 安 全漏洞	CNNVD- 202605-3690	CVE-2026- 44560	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
276	Open WebUI 安 全漏洞	CNNVD- 202605-3691	CVE-2026- 44562	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
277	Open WebUI 安	CNNVD-	CVE-2026-	中危	https://github.com/open-webui/open-webui/releases	Open

	全漏洞	202605-3692	44559		hub.com/open-webui/open-webui/releases	WebUI
278	Open WebUI 安全漏洞	CNNVD-202605-3693	CVE-2026-44558	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
279	Open WebUI 安全漏洞	CNNVD-202605-3701	CVE-2026-44550	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
280	OpenClaw 安全漏洞	CNNVD-202605-672	CVE-2026-43574	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
281	OpenClaw 安全漏洞	CNNVD-202605-673	CVE-2026-43572	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
282	OpenClaw 安全漏洞	CNNVD-202605-675	CVE-2026-43570	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
283	OpenClaw 安全漏洞	CNNVD-202605-677	CVE-2026-43567	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
284	OpenClaw 安全漏洞	CNNVD-202605-678	CVE-2026-43535	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
285	OpenClaw 安全漏洞	CNNVD-202605-680	CVE-2026-43568	中危	https://github.com/openclaw/openclaw/releases	OpenClaw

286	OpenClaw 安全漏洞	CNNVD-202605-687	CVE-2026-43528	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
287	OpenClaw 安全漏洞	CNNVD-202605-2223	CVE-2026-45005	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
288	OpenClaw 安全漏洞	CNNVD-202605-2225	CVE-2026-45002	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
289	OpenClaw 代码问题漏洞	CNNVD-202605-2227	CVE-2026-45000	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
290	OpenClaw 数据伪造问题漏洞	CNNVD-202605-2228	CVE-2026-44999	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
291	OpenClaw 安全漏洞	CNNVD-202605-696	CVE-2026-42433	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
292	OpenClaw 安全漏洞	CNNVD-202605-2229	CVE-2026-45003	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
293	OpenClaw 安全漏洞	CNNVD-202605-2230	CVE-2026-44998	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
294	OpenClaw 安全漏洞	CNNVD-202605-2231	CVE-2026-44997	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
295	OpenClaw 安全漏洞	CNNVD-202605-2235	CVE-2026-44994	中危	https://github.com/openclaw/openclaw/releases	OpenClaw

					nclaw/openc law/release s	
296	OpenClaw 安全 漏洞	CNNVD- 202605-2236	CVE-2026- 44992	中危	https://git hub.com/ope nclaw/openc law/release s	OpenClaw
297	OpenClaw 安全 漏洞	CNNVD- 202605-2237	CVE-2026- 44991	中危	https://git hub.com/ope nclaw/openc law/release s	OpenClaw
298	OpenClaw 安全 漏洞	CNNVD- 202605-2240	CVE-2026- 44993	中危	https://git hub.com/ope nclaw/openc law/release s	OpenClaw
299	Syft 安全漏洞	CNNVD- 202605-2763	CVE-2026- 31220	中危	https://git hub.com/Ope nMined/PySy ft/releases	OpenMined
300	ProcessMaker 安全漏洞	CNNVD- 202605-3857	CVE-2021- 47978	中危	https://www .processmak er.com/	ProcessMa ker
301	New API 代码问 题漏洞	CNNVD- 202605-1478	CVE-2026- 42339	中危	https://git hub.com/Qua ntumNous/ne w- api/release s/	QuantumNo us
302	Quarkus OpenAPI Generator 信息 泄露漏洞	CNNVD- 202605-1893	CVE-2026- 42333	中危	https://git hub.com/qua rkiverse/qua rkus- openapi- generator/r eleases	Quarkiver se Hub
303	Ray 代码注入漏 洞	CNNVD- 202605-1499	CVE-2026- 41486	中危	https://git hub.com/ray - project/ray /releases/	ray- project
304	sglang 注入漏 洞	CNNVD- 202605-268	CVE-2026- 7669	中危	https://git hub.com/sgl - project/sgl	sgl- project

					ang/releases	
305	Mamba 安全漏洞	CNNVD-202605-2689	CVE-2026-31239	中危	https://github.com/state-spaces/mamba/releases	state-spaces
306	superduper 安全漏洞	CNNVD-202605-2756	CVE-2026-31225	中危	https://github.com/superduper-io/superduper/releases	superduper.io
307	Toeverything AFFiNE 授权问题漏洞	CNNVD-202605-346	CVE-2026-7702	中危	https://affine.pro/	Toeverything
308	cognee 安全漏洞	CNNVD-202605-2697	CVE-2026-31231	中危	https://github.com/topoteretes/cognee/releases	Topoteretes
309	Universal Tool Calling Protocol 安全漏洞	CNNVD-202605-3391	CVE-2026-45370	中危	https://www.utcp.io/	Universal Tool Calling Protocol
310	Universal Tool Calling Protocol 代码问题漏洞	CNNVD-202605-3396	CVE-2026-44661	中危	https://www.utcp.io/	Universal Tool Calling Protocol
311	Universal Tool Calling Protocol 操作系统命令注入漏洞	CNNVD-202605-3401	CVE-2026-45369	中危	https://www.utcp.io/	Universal Tool Calling Protocol
312	V2Board SQL 注入漏洞	CNNVD-202605-058	CVE-2026-37505	中危	https://github.com/v2board/v2board	V2Board
313	V2Board 安全漏洞	CNNVD-202605-061	CVE-2026-37504	中危	https://github.com/v2board/v2board	V2Board
314	PageIndex 安全漏洞	CNNVD-202605-2202	CVE-2026-8318	中危	https://github.com/VectifyAI/PageIndex/	Vectify AI
315	vercel 信息泄露漏洞	CNNVD-202605-3116	CVE-2026-44479	中危	https://github.com/ver	Vercel

					cel/vercel/ releases	
316	AI SDK 命令注入漏洞	CNNVD- 202605-3901	CVE-2026- 8767	中危	https://github.com/vercel/ai/releases	Vercel
317	Vercel AI SDK 资源管理错误漏洞	CNNVD- 202605-3905	CVE-2026- 8769	中危	https://github.com/vercel/ai/releases	Vercel
318	Verint Verba 跨站脚本漏洞	CNNVD- 202605-3524	CVE-2026- 21730	中危	https://get.vitalsource.com/what-we-offer/verba	Verint
319	vLLM 安全漏洞	CNNVD- 202605-2498	CVE-2026- 44223	中危	https://github.com/vllm-project/vllm/releases	vLLM
320	vLLM 输入验证错误漏洞	CNNVD- 202605-2499	CVE-2026- 44222	中危	https://github.com/vllm-project/vllm/releases	vLLM
321	VMware Spring AI 安全漏洞	CNNVD- 202605-1943	CVE-2026- 41705	中危	https://github.com/spring-projects/spring-ai/releases	VMware
322	MiniClaw 命令注入漏洞	CNNVD- 202605-2010	CVE-2026- 8235	中危	https://github.com/8421bit/MiniClaw/	个人开发者
323	n8n-MCP 日志信息泄露漏洞	CNNVD- 202605-1503	CVE-2026- 42282	中危	https://github.com/czlonkowski/n8n-mcp/releases	个人开发者
324	n8n-MCP 安全漏洞	CNNVD- 202605-1508	CVE-2026- 44694	中危	https://github.com/czlonkowski/n8n-mcp/releases	个人开发者

325	n8n-MCP 日志信息泄露漏洞	CNNVD-202605-1511	CVE-2026-41495	中危	https://github.com/czlonkowski/n8n-mcp/releases	个人开发者
326	MiniClaw 路径遍历漏洞	CNNVD-202605-1260	CVE-2026-8113	中危	https://github.com/8421bit/MiniClaw/	个人开发者
327	MiniClaw 命令注入漏洞	CNNVD-202605-1262	CVE-2026-8112	中危	https://github.com/8421bit/MiniClaw/	个人开发者
328	Hermes Web UI 路径遍历漏洞	CNNVD-202605-3055	CVE-2026-22677	中危	https://github.com/nescuena/hermes-webui/releases/	个人开发者
329	ZMCPTools 路径遍历漏洞	CNNVD-202604-5871	CVE-2026-7445	中危	https://github.com/ZachHandley/ZMCPTools/	个人开发者
330	Wireshark MCP 路径遍历漏洞	CNNVD-202605-2052	CVE-2026-43901	中危	https://github.com/bx33661/Wireshark-MCP/releases	个人开发者
331	Word Tools MCP Server 路径遍历漏洞	CNNVD-202605-520	CVE-2026-7738	中危	https://github.com/pucunhunje/doc-tools-mcp/	个人开发者
332	The Ultimate Mathematical & AI Toolkit 路径遍历漏洞	CNNVD-202605-269	CVE-2026-7645	中危	https://github.com/ruvnet/subline-artime-solver/	个人开发者
333	Rijksmuseum MCP Server 命令注入漏洞	CNNVD-202605-271	CVE-2026-7653	中危	https://github.com/rhuijts/rijksmuseum-mcp	个人开发者
334	Astro MCP Server 注入漏洞	CNNVD-202605-016	CVE-2026-7591	中危	https://github.com/TimBroddin/astro-mcp-	个人开发者

					server/	
335	Code Runner MCP Server 访问控制错误漏洞	CNNVD- 202605-2832	CVE-2026- 5029	中危	https://github.com/for-mulahendry/mcp-server-code-runner	个人开发者
336	AI Development Assistant MCP Server 注入漏洞	CNNVD- 202605-277	CVE-2026- 7629	中危	https://github.com/kleneway/awesome-cursor-mcp-server	个人开发者
337	Coding Standards MCP Server 路径遍历漏洞	CNNVD- 202605-022	CVE-2026- 7588	中危	https://github.com/ggerve/coding-standards-mcp	个人开发者
338	Test Runner MCP 命令注入漏洞	CNNVD- 202605-540	CVE-2026- 7730	中危	https://github.com/priusim/mcp-test-runner	个人开发者
339	Directus MCP Server 代码问题漏洞	CNNVD- 202605-542	CVE-2026- 7729	中危	https://github.com/pixelsock/directus-mcp/	个人开发者
340	MCP-RTFM 路径遍历漏洞	CNNVD- 202605-545	CVE-2026- 7728	中危	https://github.com/ryanjoachim/mcp-rtfm/	个人开发者
341	MCP Server for ArangoDB 路径遍历漏洞	CNNVD- 202605-558	CVE-2026- 7715	中危	https://github.com/ravenwits/mcp-server-arangodb/	个人开发者
342	xiaozhi-mcphub 路径遍历漏洞	CNNVD- 202605-1875	CVE-2026- 8116	中危	https://github.com/huangjunsen0406/xiaozhi-mcphub/releases	个人开发者
343	open-notebook 安全漏洞	CNNVD- 202605-1382	CVE-2026- 33589	中危	https://github.com/lfnovo/open-notebook/releases	个人开发者
344	tgpt 注入漏洞	CNNVD- 202605-1912	CVE-2026- 8210	中危	https://github.com/aandrew-	个人开发者

					me/tgpt	
345	phpMyFAQ 安全漏洞	CNNVD-202605-3710	CVE-2026-46365	中危	https://www.phpmyfaq.de/	个人开发者
346	phpMyFAQ 跨站脚本漏洞	CNNVD-202605-3711	CVE-2026-46363	中危	https://www.phpmyfaq.de/	个人开发者
347	phpMyFAQ 安全漏洞	CNNVD-202605-3713	CVE-2026-46362	中危	https://www.phpmyfaq.de/	个人开发者
348	phpMyFAQ 跨站脚本漏洞	CNNVD-202605-3714	CVE-2026-46361	中危	https://www.phpmyfaq.de/	个人开发者
349	LLM 安全漏洞	CNNVD-202605-2692	CVE-2026-31236	中危	https://github.com/simonw/llm/releases	个人开发者
350	phpMyFAQ 跨站脚本漏洞	CNNVD-202605-3715	CVE-2026-46360	中危	https://www.phpmyfaq.de/	个人开发者
351	imgaug 安全漏洞	CNNVD-202605-2693	CVE-2026-31235	中危	https://github.com/aleju/imgaug	个人开发者
352	phpMyFAQ 安全漏洞	CNNVD-202605-3719	CVE-2026-45010	中危	https://www.phpmyfaq.de/	个人开发者
353	phpMyFAQ 安全漏洞	CNNVD-202605-3720	CVE-2026-45009	中危	https://www.phpmyfaq.de/	个人开发者
354	phpMyFAQ 安全漏洞	CNNVD-202605-3721	CVE-2026-45008	中危	https://www.phpmyfaq.de/	个人开发者
355	phpMyFAQ 安全漏洞	CNNVD-202605-3722	CVE-2026-45007	中危	https://www.phpmyfaq.de/	个人开发者
356	PraisonAI 输入验证错误漏洞	CNNVD-202605-1686	CVE-2026-44337	中危	https://github.com/MervinPraison/PraisonAI/releases	个人开发者
357	JunoClaw 操作系统命令注入漏洞	CNNVD-202605-2718	CVE-2026-43991	中危	https://github.com/Dragonmonk111/junoclaw/releases	个人开发者
358	Inbox Zero 信	CNNVD-	CVE-2026-	中危	https://git	个人开发

	息泄露漏洞	202605-2249	42865		hub.com/eli e222/inbox- zero/releas es	者
359	Machine Learning Engineering Open Book 安全漏洞	CNNVD-202605-2768	CVE-2026-31214	中危	https://git hub.com/sta s00/ml- engineering	个人开发 者
360	JeecgBoot 注入漏洞	CNNVD-202605-1259	CVE-2026-8114	中危	https://jee cg.com/	国炬
361	JeecgBoot 代码问题漏洞	CNNVD-202605-312	CVE-2026-7605	中危	https://jee cg.com/	国炬
362	JeecgBoot 代码问题漏洞	CNNVD-202605-325	CVE-2026-7604	中危	https://jee cg.com/	国炬
363	JeecgBoot 代码问题漏洞	CNNVD-202605-326	CVE-2026-7603	中危	https://jee cg.com/	国炬
364	JeecgBoot 安全漏洞	CNNVD-202605-335	CVE-2026-7602	中危	https://jee cg.com/	国炬

（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-202605-682	超危
2	CNNVD-202605-1688	高危
3	CNNVD-202604-5679	高危

1. OpenClaw 数据伪造问题漏洞（CNNVD-202605-682）

OpenClaw 是一个开源的智能人工助理。

OpenClaw 2026.4.10 之前版本存在数据伪造问题漏洞，该漏洞源于对用户的输入验证不足，攻击者利用该漏洞可以篡改数据。

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/releases>

2. PraiseAI 输入验证错误漏洞（CNNVD-202605-1688）

PraiseAI 是一个低代码多智能体协作框架。

PraiseAI 4.6.34 之前版本存在输入验证错误漏洞，该漏洞源于 MCP 服务器中文件处理工具未对路径进行检查，攻击者利用该漏洞可以写入任意文件，并可以执行任意代码。

目前厂商已发布升级补丁以修复漏洞，参考链接：

<https://github.com/MervinPraise/PraiseAI/releases>

3. Ollama 路径遍历漏洞（CNNVD-202604-5679）

Ollama 是一个开源的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 0.12.10 版本至 0.17.5 版本存在路径遍历漏洞，该漏洞源于在构造本地文件路径时未验证路径安全性，攻击者利用该漏洞可以将文件写入任意位置。

目前厂商已发布升级补丁以修复漏洞，参考链接：

<https://ollama.com/>