

人工智能重要漏洞通报

（2026 年第四期）

根据国家信息安全漏洞库（CNNVD）统计，近期（2026 年 3 月 20 日至 2026 年 3 月 30 日）共采集重要人工智能漏洞 162 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、n8n、VMware 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 17 个，高危漏洞 49 个，中危漏洞 96 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 162 个。

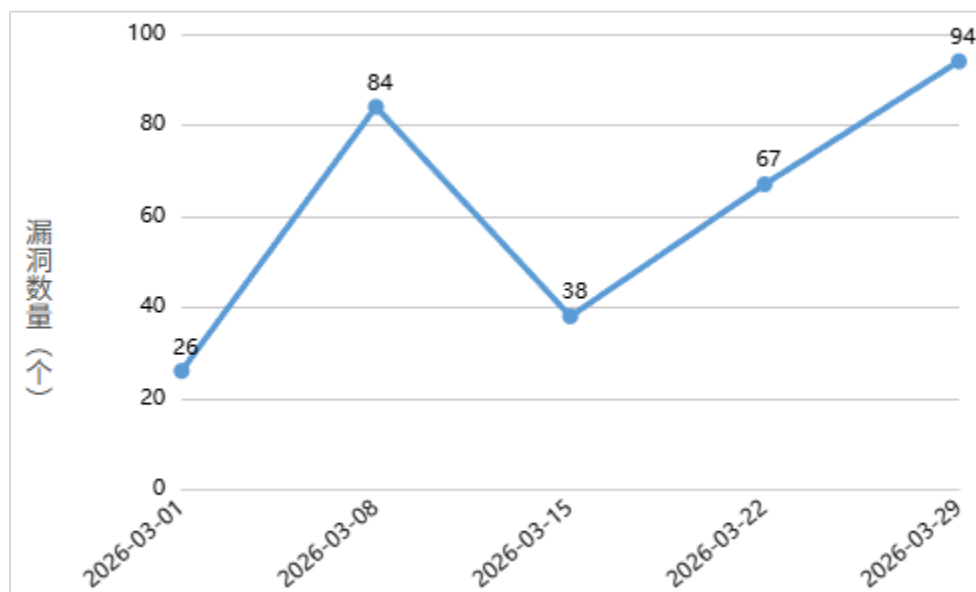


图 1 近五周漏洞新增数量统计图

（二）人工智能漏洞具体情况

近期共采集人工智能漏洞 162 个，包括 OpenClaw、n8n、VMware 等多个厂商（项目）的漏洞。其中超危漏洞 17 个，高危漏洞 49 个，中危漏洞 96 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	nanobot 安全漏洞	CNNVD-202603-5570	CVE-2026-33654	超危	https://github.com/HKUDS/nanobot/releases	Data Intelligence Lab@HKU
2	Langflow 安全漏洞	CNNVD-202603-3797	CVE-2026-33017	超危	https://github.com/langflow-ai/langflow/releases	Langflow
3	Mesop 代码注入漏洞	CNNVD-202603-3781	CVE-2026-33057	超危	https://github.com/mesop-dev/mesop/releases/	Mesop
4	MLflow 命令注入漏洞	CNNVD-202603-6017	CVE-2025-15379	超危	https://github.com/mlflow/mlflow/releases	MLflow
5	MLflow 安全漏洞	CNNVD-202603-5885	CVE-2025-15036	超危	https://github.com/mlflow/mlflow/releases	MLflow
6	n8n SQL 注入漏洞	CNNVD-202603-4693	CVE-2026-33713	超危	https://github.com/n8n-io/n8n/releases	n8n
7	n8n 安全漏洞	CNNVD-202603-4694	CVE-2026-33696	超危	https://github.com/n8n-io/n8n/releases	n8n
8	n8n 代码注入漏洞	CNNVD-202603-4696	CVE-2026-33660	超危	https://github.com/n8n-io/n8n/releases	n8n
9	n8n 安全漏洞	CNNVD-202603-4700	CVE-2026-33663	超危	https://github.com/n8n-io/n8n/releases	n8n
10	OpenClaw 安全漏洞	CNNVD-202603-5854	CVE-2026-32987	超危	https://github.com/openclaw/openclaw/releases	OpenClaw
11	OpenClaw 安全漏洞	CNNVD-202603-5855	CVE-2026-32973	超危	https://github.com/openclaw/openclaw/releases	OpenClaw
12	OpenClaw 安全漏洞	CNNVD-202603	CVE-2026-	超危	https://github.com/openclaw/openclaw/releases	OpenClaw

		-5857	32975			
13	OpenClaw 安全漏洞	CNNVD-202603-5858	CVE-2026-32924	超危	https://github.com/openclaw/openclaw/releases	OpenClaw
14	OpenClaw 安全漏洞	CNNVD-202603-5859	CVE-2026-32922	超危	https://github.com/openclaw/openclaw/releases	OpenClaw
15	OpenClaw 安全漏洞	CNNVD-202603-4168	CVE-2026-32913	超危	https://github.com/openclaw/openclaw/releases	OpenClaw
16	OpenClaw 安全漏洞	CNNVD-202603-3705	CVE-2026-22172	超危	https://github.com/openclaw/openclaw/releases	OpenClaw
17	VMware Spring AI 安全漏洞	CNNVD-202603-5743	CVE-2026-22738	超危	https://spring.io/security/cve-2026-22738	VMware
18	ApiFlow 代码问题漏洞	CNNVD-202603-3900	CVE-2026-4528	高危	https://apiflow.cn/zh	ApiFlow
19	BentoML 代码注入漏洞	CNNVD-202603-5755	CVE-2026-33744	高危	https://github.com/bentoml/BentoML/releases	BentoML
20	DB-GPT SQL 注入漏洞	CNNVD-202603-3655	CVE-2026-4504	高危	https://github.com/eosphoros-ai/DB-GPT/releases	eosphoros
21	Langflow 安全漏洞	CNNVD-202603-5544	CVE-2026-34046	高危	https://www.langflow.org/desktop	Langflow
22	Langflow 代码注入漏洞	CNNVD-202603-5554	CVE-2026-33873	高危	https://www.langflow.org/desktop	Langflow
23	Langflow 安全漏洞	CNNVD-202603-3778	CVE-2026-33053	高危	https://github.com/langflow-ai/langflow/releases	Langflow
24	Langflow 安全漏洞	CNNVD-202603-5661	CVE-2026-5027	高危	https://github.com/langflow-ai/langflow/releases	Langflow
25	Letta-ai letta 安全漏洞	CNNVD-202603-5590	CVE-2026-4965	高危	https://github.com/letta-ai/letta/releases	Letta-ai
26	LibreChat 代码问题漏洞	CNNVD-202603-5549	CVE-2026-31943	高危	https://github.com/danny-avila/LibreChat/tags	LibreChat
27	LibreChat 代码问题漏洞	CNNVD-202603-5551	CVE-2026-31945	高危	https://github.com/danny-avila/LibreChat/tags	LibreChat

28	Llama Stack 安全漏洞	CNNVD- 202603 -5271	CVE- 2025- 12805	高危	https://github.com/llama-astack/llama-stack-k8s-operator	Meta Llama
29	Mobile Next 安全漏洞	CNNVD- 202603 -5546	CVE- 2026- 33989	高危	https://github.com/mobile-next/mobile-mcp/releases	Mobile Next
30	n8n 跨站脚本 漏洞	CNNVD- 202603 -4684	CVE- 2026- 33749	高危	https://github.com/n8n-io/n8n/releases	n8n
31	n8n 授权问题 漏洞	CNNVD- 202603 -4695	CVE- 2026- 33665	高危	https://github.com/n8n-io/n8n/releases	n8n
32	NLTK 路径遍历 漏洞	CNNVD- 202603 -3604	CVE- 2026- 33236	高危	https://github.com/nltk/nltk/tags	NLTK
33	NLTK 访问控制 错误漏洞	CNNVD- 202603 -3605	CVE- 2026- 33231	高危	https://github.com/nltk/nltk/tags	NLTK
34	Open WebUI 安 全漏洞	CNNVD- 202603 -5775	CVE- 2026- 28788	高危	https://github.com/open-webui/open-webui/releases	Open WebUI
35	XAgent 访问控 制错误漏洞	CNNVD- 202603 -5647	CVE- 2026- 4959	高危	https://github.com/OpenBMB/XAgent	OpenBMB
36	OpenClaw 访问 控制错误漏洞	CNNVD- 202603 -4041	CVE- 2026- 32064	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
37	OpenClaw 操作 系统命令注入 漏洞	CNNVD- 202603 -4044	CVE- 2026- 32056	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
38	OpenClaw 安全 漏洞	CNNVD- 202603 -4048	CVE- 2026- 32051	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
39	OpenClaw 路径 遍历漏洞	CNNVD- 202603 -4051	CVE- 2026- 32055	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
40	OpenClaw 安全 漏洞	CNNVD- 202603 -4052	CVE- 2026- 32049	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
41	OpenClaw 安全 漏洞	CNNVD- 202603 -4053	CVE- 2026- 32048	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
42	OpenClaw 安全 漏洞	CNNVD- 202603 -5847	CVE- 2026- 33575	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
43	OpenClaw 安全	CNNVD-	CVE-	高危	https://github.com/open	OpenClaw

	漏洞	202603-5849	2026-33572		claw/openclaw/releases	
44	OpenClaw 安全漏洞	CNNVD-202603-5850	CVE-2026-33573	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
45	OpenClaw 安全漏洞	CNNVD-202603-4059	CVE-2026-32042	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
46	OpenClaw 安全漏洞	CNNVD-202603-5851	CVE-2026-32980	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
47	OpenClaw 安全漏洞	CNNVD-202603-5852	CVE-2026-32978	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
48	OpenClaw 安全漏洞	CNNVD-202603-5853	CVE-2026-32979	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
49	OpenClaw 数据伪造问题漏洞	CNNVD-202603-5856	CVE-2026-32974	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
50	OpenClaw 安全漏洞	CNNVD-202603-5862	CVE-2026-32915	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
51	OpenClaw 安全漏洞	CNNVD-202603-5865	CVE-2026-32918	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
52	OpenClaw 安全漏洞	CNNVD-202603-5866	CVE-2026-32914	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
53	OpenClaw 安全漏洞	CNNVD-202603-5880	CVE-2026-32972	高危	https://github.com/openclaw/openclaw/releases	OpenClaw
54	OpenHands 操作系统命令注入漏洞	CNNVD-202603-5764	CVE-2026-33718	高危	https://github.com/OpenHands/OpenHands/releases	OpenHands
55	PandasAI 代码注入漏洞	CNNVD-202603-5798	CVE-2026-4998	高危	https://github.com/sinaptik-ai/pandas-ai/releases	PandasAI
56	vLLM 安全漏洞	CNNVD-202603-5777	CVE-2026-27893	高危	https://github.com/vllm-project/vllm/releases	vLLM
57	VMware Spring AI 安全漏洞	CNNVD-202603-5740	CVE-2026-22744	高危	https://spring.io/security/cve-2026-22744	VMware
58	LocalGPT 安全漏洞	CNNVD-202603	CVE-2026-	高危	https://github.com/promtengineer/localgpt	个人开发者

		-5794	5002			
59	LocalGPT 代码问题漏洞	CNNVD-202603-5795	CVE-2026-5001	高危	https://github.com/promtengineer/localgpt	个人开发者
60	LocalGPT 访问控制错误漏洞	CNNVD-202603-5796	CVE-2026-5000	高危	https://github.com/promtengineer/localgpt	个人开发者
61	Azure Data Explorer MCP Server 安全漏洞	CNNVD-202603-5541	CVE-2026-33980	高危	https://github.com/pablito0/adx-mcp-server/releases	个人开发者
62	PandasAI SQL 注入漏洞	CNNVD-202603-5800	CVE-2026-4996	高危	https://github.com/sinaptik-ai/pandas-ai/releases	个人开发者
63	LoLLMs 安全漏洞	CNNVD-202603-5839	CVE-2026-0562	高危	https://github.com/ParisNeo/lollms/releases	个人开发者
64	LoLLMs 代码问题漏洞	CNNVD-202603-5840	CVE-2026-0560	高危	https://github.com/ParisNeo/lollms/releases	个人开发者
65	LoLLMs 授权问题漏洞	CNNVD-202603-5843	CVE-2026-0558	高危	https://github.com/ParisNeo/lollms/releases	个人开发者
66	mcp-memory-service 安全漏洞	CNNVD-202603-3666	CVE-2026-33010	高危	https://github.com/doobido/mcp-memory-service/releases	个人开发者
67	Claude Code 安全漏洞	CNNVD-202603-3745	CVE-2026-33068	中危	https://github.com/anthropics/claude-code/releases	Anthropic
68	bagofwords 安全漏洞	CNNVD-202603-3656	CVE-2026-4500	中危	https://github.com/bagofwords1/bagofwords/releases	bagofwords1
69	DeerFlow 安全漏洞	CNNVD-202603-5704	CVE-2026-32859	中危	https://github.com/bytedance/deer-flow	Bytedance
70	Chatwoot 安全漏洞	CNNVD-202603-5565	CVE-2026-4990	中危	https://www.chatwoot.com/	Chatwoot
71	CodePhiliaX Chat2DB 代码问题漏洞	CNNVD-202603-4300	CVE-2026-4586	中危	https://github.com/CodePhiliaX/Chat2DB/releases	CodePhiliaX
72	CrewAI 安全漏洞	CNNVD-202603-5977	CVE-2026-2287	中危	https://docs.crewai.com/en/tools/ai-ml/codeinterpretertool	CrewAI
73	CrewAI 安全漏洞	CNNVD-202603	CVE-2026-	中危	https://docs.crewai.com/en/tools/ai-ml/codeinterpretertool	CrewAI

		-5978	2285		ml/codeinterpretertool	
74	CrewAI 安全漏洞	CNNVD-202603-5979	CVE-2026-2286	中危	https://docs.crewai.com/en/tools/ai-ml/codeinterpretertool	CrewAI
75	CrewAI 安全漏洞	CNNVD-202603-5980	CVE-2026-2275	中危	https://github.com/crewAIInc/crewAI/releases	CrewAI
76	SQLBot SQL 注入漏洞	CNNVD-202603-3804	CVE-2026-32950	中危	https://github.com/dataease/SQLBot/releases	DataEase
77	SQLBot 代码问题漏洞	CNNVD-202603-3805	CVE-2026-32949	中危	https://github.com/dataease/SQLBot/releases	DataEase
78	Discourse 安全漏洞	CNNVD-202603-4068	CVE-2026-33428	中危	https://github.com/discourse/discourse/tags	Discourse
79	Discourse 安全漏洞	CNNVD-202603-4069	CVE-2026-33427	中危	https://github.com/discourse/discourse/tags	Discourse
80	Discourse 安全漏洞	CNNVD-202603-4071	CVE-2026-33425	中危	https://github.com/discourse/discourse/tags	Discourse
81	Discourse 安全漏洞	CNNVD-202603-3817	CVE-2026-32114	中危	https://github.com/discourse/discourse/tags	Discourse
82	Discourse 安全漏洞	CNNVD-202603-4073	CVE-2026-33424	中危	https://github.com/discourse/discourse/tags	Discourse
83	Discourse 安全漏洞	CNNVD-202603-3827	CVE-2026-31869	中危	https://github.com/discourse/discourse/tags	Discourse
84	Discourse 安全漏洞	CNNVD-202603-3830	CVE-2026-31805	中危	https://github.com/discourse/discourse/tags	Discourse
85	Discourse 信息泄露漏洞	CNNVD-202603-3832	CVE-2026-30891	中危	https://github.com/discourse/discourse/tags	Discourse
86	Discourse 安全漏洞	CNNVD-202603-3833	CVE-2026-30889	中危	https://github.com/discourse/discourse/tags	Discourse
87	Discourse 安全漏洞	CNNVD-202603-3598	CVE-2026-33423	中危	https://github.com/discourse/discourse/tags	Discourse
88	Discourse 跨站脚本漏洞	CNNVD-202603-3600	CVE-2026-33411	中危	https://github.com/discourse/discourse/tags	Discourse

89	Discourse 安全漏洞	CNNVD-202603-3601	CVE-2026-33251	中危	https://github.com/discourse/discourse/tags	Discourse
90	Discourse 安全漏洞	CNNVD-202603-3602	CVE-2026-33291	中危	https://github.com/discourse/discourse/tags	Discourse
91	Drupal AI 安全漏洞	CNNVD-202603-5278	CVE-2026-3573	中危	https://www.drupal.org/sa-contrib-2026-028	Drupal
92	DB-GPT 代码问题漏洞	CNNVD-202603-3654	CVE-2026-4505	中危	https://github.com/eosphoros-ai/DB-GPT/releases	eosphoros
93	GitLab CodeRider-Kilo 安全漏洞	CNNVD-202603-5660	CVE-2026-30302	中危	https://coderider.gitlab.cn/en	GitLab
94	Gravity Cloud Services Axon Code 安全漏洞	CNNVD-202603-5692	CVE-2026-30303	中危	https://www.matterai.so/	Gravity Cloud Services
95	HiJiffy Chatbot 安全漏洞	CNNVD-202603-5463	CVE-2026-4263	中危	https://www.hijiffy.com/	HiJiffy
96	HiJiffy Chatbot 安全漏洞	CNNVD-202603-5464	CVE-2026-4262	中危	https://www.hijiffy.com/	HiJiffy
97	smolagents 安全漏洞	CNNVD-202603-5535	CVE-2026-4963	中危	https://github.com/huggingface/smolagents/releases	Hugging Face
98	FastGPT 安全漏洞	CNNVD-202603-3739	CVE-2026-33075	中危	https://github.com/labring/FastGPT/releases	labring
99	Langflow 安全漏洞	CNNVD-202603-5662	CVE-2026-5026	中危	https://github.com/langflow-ai/langflow/releases	Langflow
100	Langflow 安全漏洞	CNNVD-202603-5663	CVE-2026-5022	中危	https://github.com/langflow-ai/langflow/releases	Langflow
101	Langflow 安全漏洞	CNNVD-202603-5664	CVE-2026-5025	中危	https://github.com/langflow-ai/langflow/releases	Langflow
102	Letta-ai letta 安全漏洞	CNNVD-202603-5630	CVE-2026-4964	中危	https://github.com/letta-ai/letta/releases	Letta-ai
103	LibreChat 访问控制错误漏洞	CNNVD-202603-5596	CVE-2026-31950	中危	https://github.com/danny-avila/LibreChat/tags	LibreChat
104	LibreChat 信	CNNVD-	CVE-	中危	https://github.com/dann	LibreCha

	息泄露漏洞	CNNVD-202603-5608	CVE-2026-31951		y-avila/LibreChat/tags	t
105	Federated Learning and Interoperability Platform 安全漏洞	CNNVD-202603-5605	CVE-2026-33879	中危	https://github.com/londonaicentre/FLIP/releases	London AI Centre
106	Mesop 安全漏洞	CNNVD-202603-3777	CVE-2026-33054	中危	https://github.com/mesop-dev/mesop/releases/	Mesop
107	MetaGPT 安全漏洞	CNNVD-202603-3912	CVE-2026-4516	中危	https://github.com/FoundationAgents/MetaGPT/releases	MetaGPT
108	MetaGPT 代码注入漏洞	CNNVD-202603-3942	CVE-2026-4515	中危	https://github.com/FoundationAgents/MetaGPT/releases	MetaGPT
109	MindSQL SQL 注入漏洞	CNNVD-202603-3630	CVE-2026-4507	中危	https://github.com/Mindinventory/MindSQL	MindInventory
110	MindSQL 代码注入漏洞	CNNVD-202603-3631	CVE-2026-4506	中危	https://github.com/Mindinventory/MindSQL	MindInventory
111	MLflow 信息泄露漏洞	CNNVD-202603-5648	CVE-2025-15381	中危	https://github.com/mlflow/mlflow/releases	MLflow
112	MCP Ruby SDK 安全漏洞	CNNVD-202603-5579	CVE-2026-33946	中危	https://github.com/modelcontextprotocol/ruby-sdk/releases	Model Context Protocol
113	n8n 注入漏洞	CNNVD-202603-4681	CVE-2026-33751	中危	https://github.com/n8n-io/n8n/releases	n8n
114	n8n 安全漏洞	CNNVD-202603-4685	CVE-2026-33724	中危	https://github.com/n8n-io/n8n/releases	n8n
115	n8n 安全漏洞	CNNVD-202603-4686	CVE-2026-33722	中危	https://github.com/n8n-io/n8n/releases	n8n
116	n8n 安全漏洞	CNNVD-202603-4687	CVE-2026-33720	中危	https://github.com/n8n-io/n8n/releases	n8n
117	NLTK 跨站脚本漏洞	CNNVD-202603-3606	CVE-2026-33230	中危	https://github.com/nltk/nltk/tags	NLTK
118	ON24 Q&A Chat 安全漏洞	CNNVD-202603-5991	CVE-2026-3321	中危	https://www.on24.com/	ON24

119	Open WebUI 安全漏洞	CNNVD-202603-5774	CVE-2026-29070	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
120	Open WebUI 安全漏洞	CNNVD-202603-5776	CVE-2026-28786	中危	https://github.com/open-webui/open-webui/releases	Open WebUI
121	OpenClaw 安全漏洞	CNNVD-202603-4035	CVE-2026-32899	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
122	OpenClaw 安全漏洞	CNNVD-202603-4036	CVE-2026-32898	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
123	OpenClaw 访问控制错误漏洞	CNNVD-202603-4038	CVE-2026-32896	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
124	OpenClaw 安全漏洞	CNNVD-202603-4039	CVE-2026-32895	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
125	OpenClaw 安全漏洞	CNNVD-202603-4042	CVE-2026-32065	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
126	OpenClaw 安全漏洞	CNNVD-202603-4045	CVE-2026-32057	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
127	OpenClaw 安全漏洞	CNNVD-202603-4046	CVE-2026-32053	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
128	OpenClaw 后置链接漏洞	CNNVD-202603-4047	CVE-2026-32054	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
129	OpenClaw 安全漏洞	CNNVD-202603-4049	CVE-2026-32052	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
130	OpenClaw 安全漏洞	CNNVD-202603-4054	CVE-2026-32046	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
131	OpenClaw 安全漏洞	CNNVD-202603-4055	CVE-2026-32045	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
132	OpenClaw 安全漏洞	CNNVD-202603-4056	CVE-2026-32044	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
133	OpenClaw 安全漏洞	CNNVD-202603-5848	CVE-2026-33574	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
134	OpenClaw 安全	CNNVD-	CVE-	中危	https://github.com/open	OpenClaw

	漏洞	202603-4057	2026-32043		claw/openclaw/releases	
135	OpenClaw 安全漏洞	CNNVD-202603-5860	CVE-2026-32923	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
136	OpenClaw 安全漏洞	CNNVD-202603-5861	CVE-2026-32919	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
137	OpenClaw 路径遍历漏洞	CNNVD-202603-5370	CVE-2026-32846	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
138	OpenClaw 安全漏洞	CNNVD-202603-4190	CVE-2026-27646	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
139	OpenClaw 安全漏洞	CNNVD-202603-4193	CVE-2026-27183	中危	https://github.com/openclaw/openclaw/releases	OpenClaw
140	PandasAI 路径遍历漏洞	CNNVD-202603-5799	CVE-2026-4997	中危	https://github.com/sinaptik-ai/pandas-ai/releases	PandasAI
141	pinchtab 代码问题漏洞	CNNVD-202603-3731	CVE-2026-33081	中危	https://github.com/pinchtab/pinchtab/releases	Pinchtab
142	HAI Builds Code Generator 安全漏洞	CNNVD-202603-5916	CVE-2026-30308	中危	https://www.presidio.com/solutions/hai-build/	Presidio INC
143	PyTorch 代码问题漏洞	CNNVD-202603-4128	CVE-2026-4538	中危	https://pytorch.org/	PyTorch
144	Roo Code 安全漏洞	CNNVD-202603-5929	CVE-2026-30307	中危	https://roocode.com/	Roo Code
145	Streamlit 代码问题漏洞	CNNVD-202603-5257	CVE-2026-33682	中危	https://github.com/streamlit/streamlit/releases	Streamlit
146	SyncFusion 安全漏洞	CNNVD-202603-3663	CVE-2025-63260	中危	https://www.syncfusion.com/	SyncFusion
147	Syntx 安全漏洞	CNNVD-202603-5930	CVE-2026-30305	中危	https://github.com/OrangeCatTechnologies/SyntX	Syntx
148	Vanna SQL 注入漏洞	CNNVD-202603-3944	CVE-2026-4513	中危	https://vanna.ai/	Vanna
149	Vanna 安全漏洞	CNNVD-	CVE-	中危	https://vanna.ai/	Vanna

	洞	202603-3945	2026-4511			
150	VMware Spring AI 安全漏洞	CNNVD-202603-5741	CVE-2026-22743	中危	https://spring.io/security/cve-2026-22743	VMware
151	VMware Spring AI 安全漏洞	CNNVD-202603-5742	CVE-2026-22742	中危	https://spring.io/security/cve-2026-22742	VMware
152	OpenUI 代码注入漏洞	CNNVD-202603-5558	CVE-2026-4992	中危	https://openui.fly.dev/	Weights & Biases
153	mcp-docs-rag MCP Server 操作系统命令注入漏洞	CNNVD-202603-5790	CVE-2026-5007	中危	https://github.com/kazuiph/mcp-docs-rag/	个人开发者
154	LocalGPT 访问控制错误漏洞	CNNVD-202603-5793	CVE-2026-5003	中危	https://github.com/promtengineer/localgpt	个人开发者
155	Codebase MCP 操作系统命令注入漏洞	CNNVD-202603-5876	CVE-2026-5023	中危	https://github.com/DeDeveloper23/codebase-mcp	个人开发者
156	Cline 安全漏洞	CNNVD-202603-5914	CVE-2026-30313	中危	https://github.com/necboy/cline-DSAI	个人开发者
157	SakaDev 安全漏洞	CNNVD-202603-5919	CVE-2026-30306	中危	https://github.com/rahmanazhar/SakaDev	个人开发者
158	Aix-DB SQL 注入漏洞	CNNVD-202603-4148	CVE-2026-4530	中危	https://github.com/apconw/Aix-DB/releases	个人开发者
159	AI Code 安全漏洞	CNNVD-202603-5691	CVE-2026-30304	中危	https://marketplace.visualstudio.com/items?itemName=tianguaduizhang.claude-dev-china	个人开发者
160	Awesome LLM Apps 安全漏洞	CNNVD-202603-5693	CVE-2026-29871	中危	https://github.com/Shubhamsaboo/awesome-llm-apps	个人开发者
161	consult-llm-mcp 操作系统命令注入漏洞	CNNVD-202603-5946	CVE-2026-5125	中危	https://github.com/rainee/consult-llm-mcp/releases	个人开发者
162	Awesome LLM Apps 安全漏洞	CNNVD-202603-5956	CVE-2026-29872	中危	https://www.theunwindai.com/	个人开发者

（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-202603-5855	超危
2	CNNVD-202603-3797	超危
3	CNNVD-202603-5885	超危

1. OpenClaw 安全漏洞（CNNVD-202603-5855）

OpenClaw 是一个开源的智能人工助理。

OpenClaw 2026.3.11 之前版本存在安全漏洞，该漏洞源于 matchesExecAllowlistPattern 函数对参数进行了错误的规范化，使用了小写字母和通配符匹配，导致 POSIX 路径上出现过度匹配，攻击者利用该漏洞可以执行任意命令。

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. Langflow 安全漏洞（CNNVD-202603-3797）

Langflow 是一个用于构建多代理和 RAG 应用程序的可视化框架。

Langflow 1.9.0 之前版本存在安全漏洞，该漏洞源于没有强制进行身份验证，攻击者利用该漏洞可以远程执行代码。

目前厂商已发布升级补丁以修复漏洞，参考链接：

<https://github.com/langflow-ai/langflow/releases>

3. MLflow 安全漏洞（CNNVD-202603-5885）

MLflow 是一个开源的简化机器学习开发平台。

MLflow 3.7.0 之前版本存在安全漏洞，该漏洞源于 `extract_archive_to_dir` 函数未验证输入路径，攻击者利用该漏洞可以覆盖任意文件或提升权限。

目前厂商已发布升级补丁以修复漏洞，参考链接：

<https://github.com/mlflow/mlflow/releases>