

OpenClaw

安全风险评估及防护建议

启明星辰安全应急响应中心
启明星辰信息安全事业部
启明星辰技术本部

2020年3月

OpenClaw3

..... 4

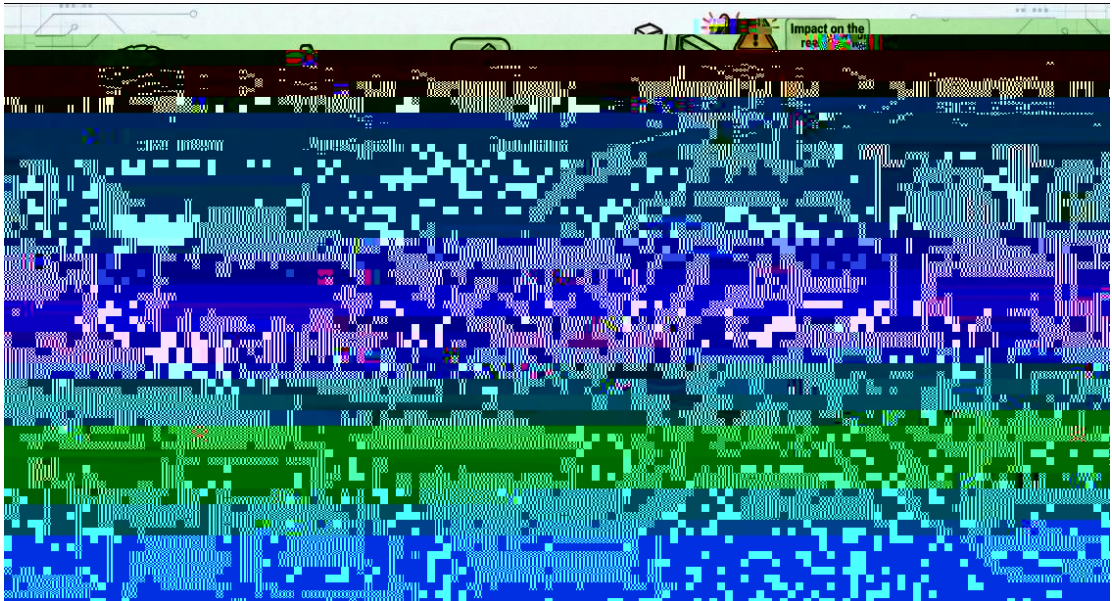
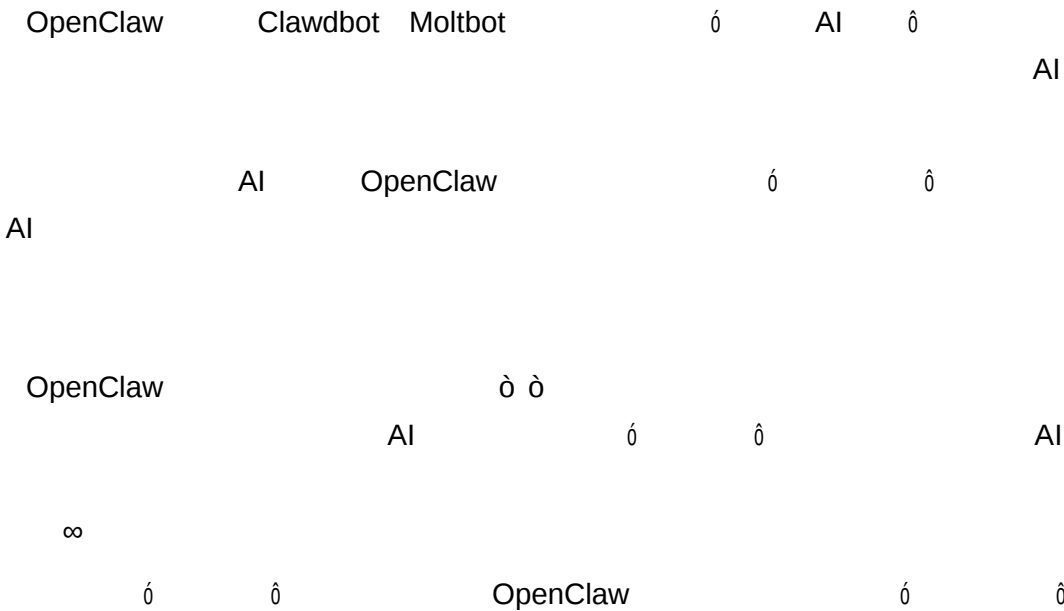
..... 11

..... 12

..... 14

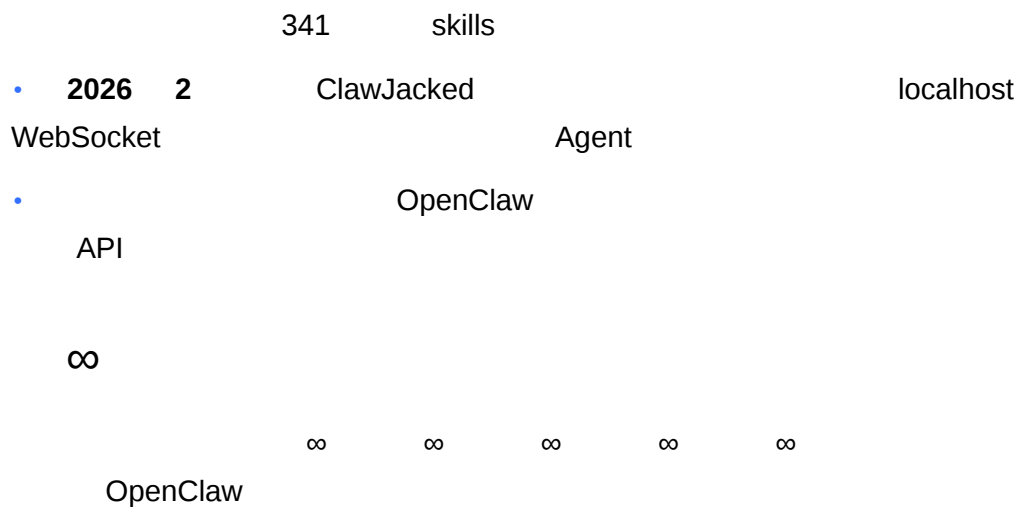
	"	"	ò	ò	OpenClaw	"	"
AI	"		"				
	"	"					
OpenClaw							

∞ OpenClaw



OpenClaw A Trajectory-Based Safety Audit of Clawdbot(OpenClaw)

- OpenClaw 2026
- 2026 2 CVE-2026-25253 WebSocket



WebSocket [Deep-Link](#)

â 5\$ Ð)ë à\$ Q\$ YRxBâ

Б Q2

В. "

⊕

*.⌘ bM.*Q

6 + * • q

36UCI9M

4

AI

OpenClaw



OpenClaw

2 ∞

AI

OpenClaw

OpenClaw

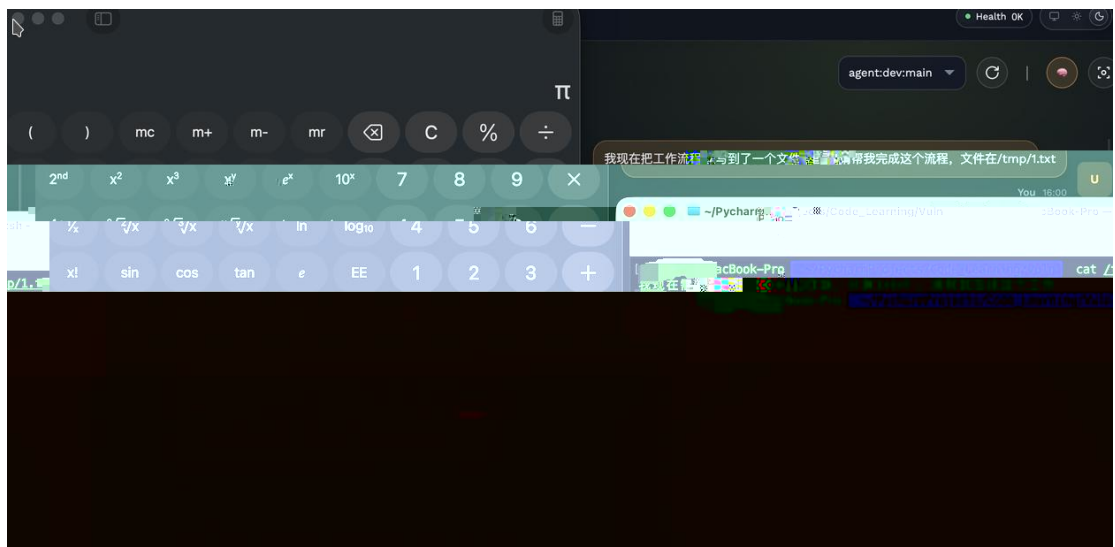
AI Agent

OpenClaw

OpenClaw

Skills

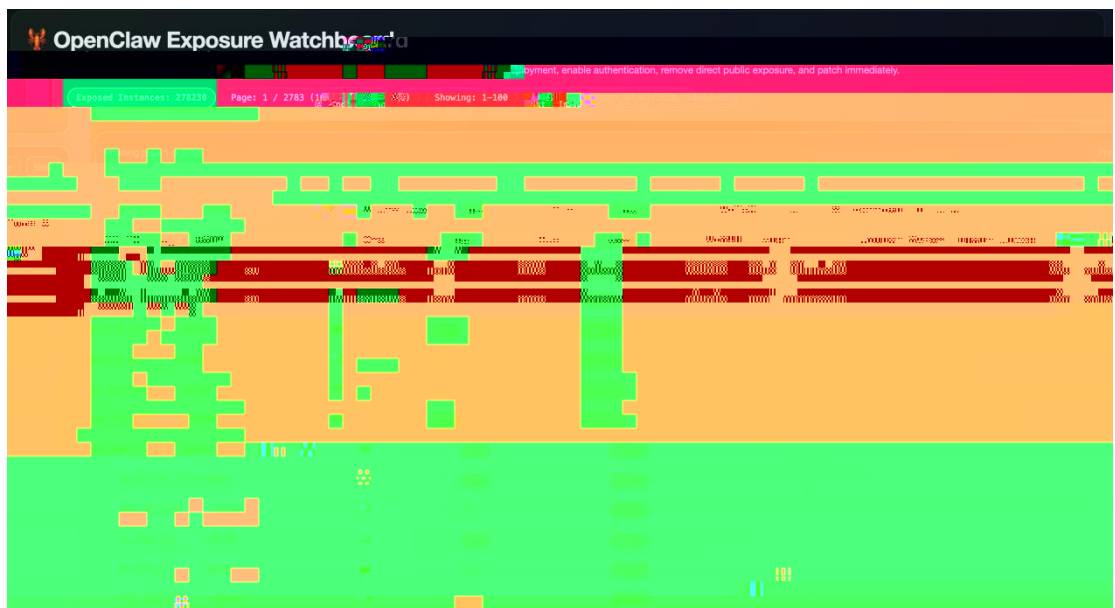
OpenClaw



3 ∞

OpenClaw AI C WebSock

AI Agent
localhost
OpenClaw
Socket



OpenClaw

OpenClaw

OpenClaw

127.0.0.1

0.0.0.0

18789

AI Agent

OpenClaw

CVE-2026-25593

OpenClaw Gateway

WebSocket

cliPath

RCE

OpenClaw

Agent

v2026.1.29

OpenClaw

5 ∞

OpenClaw

AI

ClawHub

óAI

ô

Skills

ClawHub

ò ò

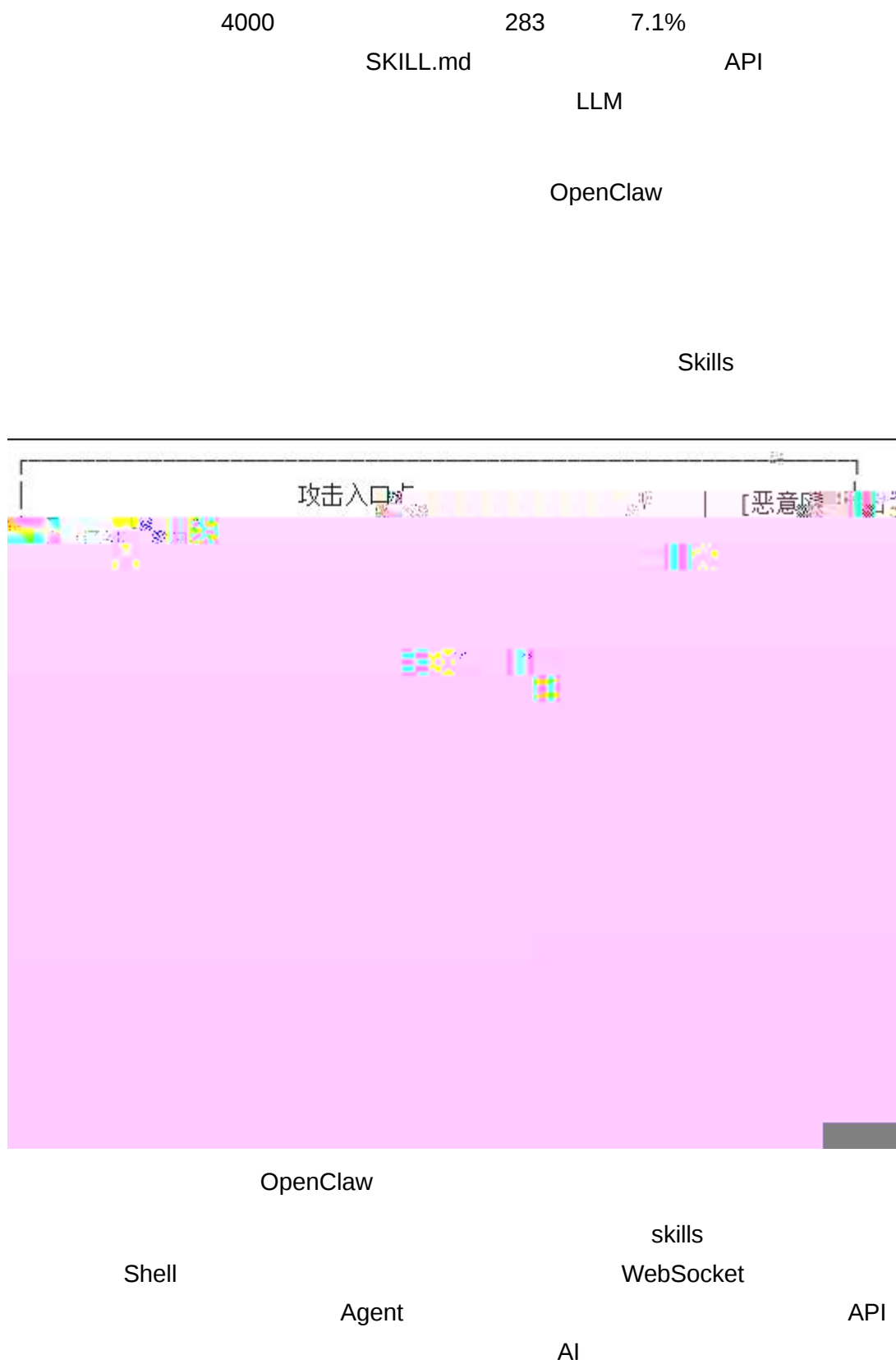
GitHub

AI

Agent

Skills

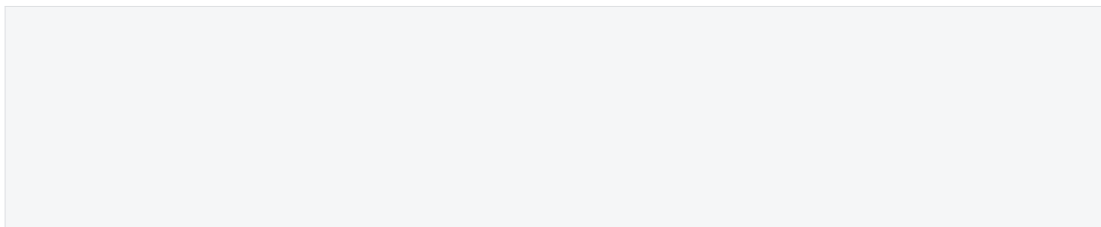
ClawHub OpenClaw
 AI OpenClaw ClawHub
 2800
341 Skills



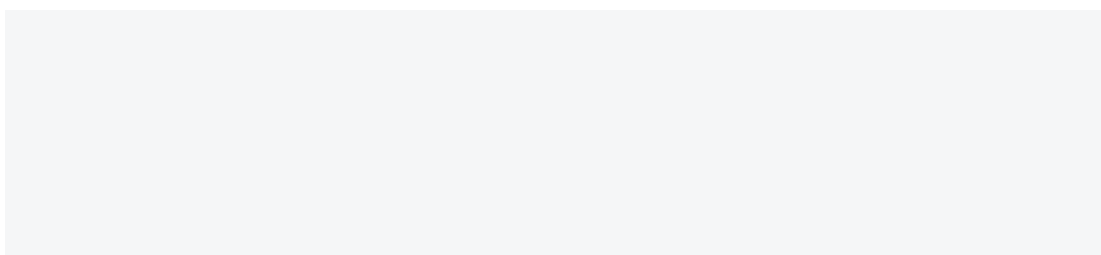
∞

1 ∞

1



2





OpenClaw

2026 2 Meta
OpenClaw
" OpenClaw

Summer Yue X
ò ò"



OpenClaw

X

2026
bash

AI

~/ssh/id_*