OpenClaw Three Months Later: 3.2 Million Users, Nine CVEs, and an OpenAI Acquisition

Kabui, Charles

2026-05-02

Three months after its viral launch as "Moltbot", OpenClaw has 3.2 million active users, 38 million monthly website visitors, and an acquisition by OpenAI. Creator Peter Steinberger joined OpenAI in February 2026 to lead agent efforts, and the project moved to independent foundation governance. NVIDIA built NemoClaw, an enterprise security stack, on top of it. The ClawHub marketplace grew to 52,700+ skills with 12 million downloads. But the growth

came with serious damage. CVE-2026-25253 scored 8.8 on CVSS and allowed one-click remote code execution. Between March 18 and 21, nine more CVEs dropped in four days, one scoring 9.9. SecurityScorecard found 135,000 exposed instances across 82 countries, with over 50,000 directly vulnerable. Over 800 malicious skills (roughly 20% of the registry) were identified in ClawHub, designed to steal API keys and credentials. The Moltbook social network for agents leaked 1.5 million API tokens and 35,000 email addresses.

Public opinion is sharply divided. Tech enthusiasts treat OpenClaw as a "cowboy-style playground" for real AI agency. Cybersecurity experts call it a nightmare, with Kaspersky finding 512 vulnerabilities in a single audit. Forbes reported widespread user frustration: setup takes days, the agent enters unnecessary reasoning loops, and tasks often fail silently. The Dutch Data Protection Authority issued a formal warning. The consensus across reviews is to avoid running it on your main machine and treat it as an experimental sandbox, not a production tool.

OpenClaw proves that consumer demand for personal AI agents is real, but the security model for always-on agents with access to messaging apps, files, and shell commands does not exist yet. The project ships patches fast (13 releases in March alone), but most users never apply them. Chinese authorities restricted it on government computers. The gap between what OpenClaw promises and what it can safely deliver remains the defining tension of the agent era.

Sources:

- OpenClaw Security Crisis (Reco AI)
- OpenClaw Security Crisis (Conscia)
- Problems With OpenClaw? You're Not Alone (Forbes)
- OpenClaw Vulnerabilities (Kaspersky)
- OpenClaw Statistics 2026
