儒风副刊

微信公众号

济宁晚报

2026年3月16日 星期一
丙午年正月廿八
今日8版 第3662期
济宁日报社主管主办
国内统一连续出版物号:CN37-0086

触摸济宁的文化脉搏

OpenClaw走红

一只“龙虾”的潜力与风险

2026年开年以来,一款名为OpenClaw的开源人工智能体(AI智能体)在全球科技圈迅速走红。这类能够在现实世界执行任务、代表用户采取行动的AI工具开始进入公众视野,引发广泛关注。

上线仅两个多月获得30万颗“星标”

OpenClaw由奥地利软件工程师彼得·施泰因贝格尔开发,是一款开源AI智能体软件。与传统聊天机器人不同,该智能体可通过整合调用通信软件和大语言模型,在用户本地电脑自主执行文件管理、邮件收发、数据处理等复杂任务。此外,用户还可以通过安装技能包代码来训练和扩展其能力。

公开数据显示,OpenClaw在开源平台GitHub上线仅两个多月便获得超过30万颗“星标”。这一指标通常被视为开源项目受欢迎程度的重要参考,显示出开发者社区对其高度关注。

美国科技媒体普遍认为,这种“能够行动的AI智能体”代表了AI发展的新方向,可能改变人与计算机的交互方式。通过连接电子邮件、日程安排和各类软件系统,AI可以自动完成一系列复杂任务,从而提升个人和企业的工作效率。

安全性和可靠性存隐忧

OpenClaw快速走红也引发安全专家和媒体的警惕。美国媒体认为,这类AI智能体需要较高系统权限才能执行任务,如访问文件、运行程序或连接用户账户,配置不当可能导致数据泄露甚至被恶意利用。

美国《福布斯》杂志网站援引研究人员观点说,AI智能体之所以引发安全担忧,是因为其同时具备三种高风险特征,即能够自主执行任务的自动化系统、可能隐藏恶意指令的信息来源,以及对用户设备拥有较高权限的访问能力。

据科技媒体平台TechRadar报道,安全研究人员发现OpenClaw的核心系统存在一个名为“ClawJacked”的重大安全漏洞,攻击者可能通过恶意网页接管AI智能体,从而获取设备权限和访问系统数据。

使用门槛较高,不适合普通用户

除了安全问题,不少用户还表示OpenClaw的使用门槛较高。有用户在美国红迪网站等技术论坛上发帖,称安装OpenClaw的过程堪称“噩梦”,各种兼容性问题和报错让人最终放弃使用。还有用户表示,OpenClaw运行环境复杂,稳定性不足,使用体验“太贵、太慢且不够可靠”。

美国科技新闻媒体TechCrunch报道说,OpenClaw安全配置和操作需要较高技术能力,目前该工具更适合技术人员或开发者使用,并不适合普通公众用户。

总体来看,美国媒体和技术社区普遍认为,OpenClaw代表了AI发展的重要方向——从“对话型AI”向“行动型AI”转变,然而,这类技术仍处于早期发展阶段,其安全性、稳定性以及监管框架仍有待进一步完善。

(来源:新华社)

图片由AI生成