“龙虾”爆火之后 为何引发广泛警惕

今年年初以来,一款俗称“龙虾”的人工智能(AI)智能体工具“开放之爪”(OpenClaw)凭借其自主执行复杂任务、可扩展技能包等强大能力,在开源社区迅速崛起。但爆火之后,“开放之爪”接连被曝出存在多重安全隐患。

目前,多国监管机构和科技企业已陆续发布针对“开放之爪”的使用指南和规范。4月1日,中国国家知识产权局发布风险提示说,“开放之爪”等智能体工具被曝光默认安全配置脆弱,易引发严重安全风险。与此同时,使用此类智能体撰写专利申请文件,也可能诱发多重风险。

“龙虾”(OpenClaw)凭借其自主执行复杂任务、可扩展技能包等强大能力,在开源社区迅速崛起。(CFP)

安全漏洞频发

“开放之爪”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。该智能体采用层级化架构,将社交即时通讯软件与自动化智能体深度耦合,同时借助插件系统扩展各种工具能力。这种分层架构虽赋予了“开放之爪”灵活性与可扩展性,但也带来了多维度的安全风险。

1月下旬,开源平台GitHub上发布的一项安全审计报告显示,“开放之爪”存在512项安全漏洞,其中有8项被归类为“严重”,涵盖了身份验证、机密管理等领域。

2月下旬,国际网络安全机构“绿洲安全”研究人员发布报告说,“开放之爪”核心系统中存在一个名为“ClawJacked”的重大安全漏洞,攻击者可能通过恶意网页接管该智能体,从而获取设备权限和访问系统数据。“开放之爪”团队将漏洞定级为“高度危险”,并在24小时内发布了修复版本。

3月30日,中国360数字安全集团在官方微信公众号上发文说,在“开放之爪”平台中发现一处高危漏洞,影响范围覆盖全球50多个国家和地区。

广泛的攻击风险

美国微软公司安全团队发布的风险报告显示,使用“开放之爪”可能面临两类攻击风险:恶意技能插件和间接提示词注入。

“开放之爪”的执行能力依赖于社区平台提供的技能插件。绿盟科技公司近期发布的安全报告指出,如果缺乏严格的代码审计和签名校验,攻击者可通过发布包含恶意提示词和代码的恶意技能插件实现“代码投毒”。用户可能只因一次点击就加载了此类插件,攻击者可在受害者系统中获得持久驻留能力。而攻击者上传自定义技能插件的门槛非常低,只需要注册一个非实名的GitHub账号即可。

据美国派拓网络公司2月发布的数据,研究人员已在相关平台上发现超过800个针对“开放之爪”的恶意技能插件。

提示词注入是一种针对大语言模型的攻击技术,分为直接注入(攻击者直接输入恶意指令)和间接注入(通过网页、文档等外部数据源实现攻击)两种方式。

美国“众击”网络安全服务公司近期在官网发文说,提示词注入的首要威胁是敏感数据泄露,考虑到“开放之爪”对敏感文件与系统的高访问权限,这一风险尤为严重。间接注入则会进一步放大风险,因为攻击者无需直接与“开放之爪”交互,只需污染其读取的数据,恶意指令即可悄悄进入软件决策流程。

多国机构及企业发布使用规范

对于“开放之爪”是否适合在企业中部署应用,“众击”公司的文章指出,若员工在企业设备上部署“开放之爪”或将其接入企业系统,且配置不当、缺乏安全保护,它就可能成为系统“后门”,执行攻击者的指令。

业内人士建议,个人或企业用户不要在常规办公与涉密设备上运行“开放之爪”,如需部署须采取权限治理、沙箱机制、持续监控与全周期安全防护等严格管控措施。

据媒体报道,出于风险管控的考虑,美国元宇宙平台公司、韩国多音通讯公司等多国科技企业已禁止员工在办公设备上使用“开放之爪”。与此同时,多国监管机构也发布了关于使用“开放之爪”的安全指南。

荷兰数据保护局2月发布公报,建议用户和组织不要在存有敏感或机密数据(如访问码、财务行政资料、员工数据、私人文档或身份证明文件)的系统上使用“开放之爪”及类似AI智能体;建议谨慎对待外部插件,实施严格的访问控制,在存在泄露风险时及时更新登录信息。该监管机构还呼吁将“开放之爪”等AI智能体纳入欧盟《人工智能法》的管辖范围。

3月22日,中国国家互联网应急中心等发布了“开放之爪”安全使用实践指南。此前,工业和信息化部网络安全威胁和漏洞信息共享平台组织相关机构研提了“六要六不要”建议,以防范“开放之爪”开源智能体安全风险。(新华)

中国大唐集团有限公司原党组副书记、总经理

寇伟一审被判死缓

2026年4月1日,内蒙古自治区兴安盟中级人民法院一审公开宣判中国大唐集团有限公司原党组副书记、总经理寇伟受贿、利用影响力受贿、贪污、国有公司人员滥用职权一案,对寇伟以受贿罪判处死刑,缓期二年执行,剥夺政治权利终身,并处没收个人全部财产;以贪污罪判处有期徒刑十二年,并处罚金人民币三百万元;以利用影响力受贿罪判处有期徒刑八年,并处罚金人民币一百万元;以国有公司人员滥用职权罪判处有期徒刑四年;决定执行死刑,缓期二年执行,剥夺政治权利终身,并处没收个人全部财产。对追缴在案的寇伟受贿、利用影响力受贿所得及孳息依法上缴国库,不足部分继续追缴;贪污所得依法返还被害单位。

经审理查明:1996年至2024年,被告人寇伟利用担任云南省漫湾发电厂党委书记、厂长,云南省电力工业局党组成员、副局长,云南电力集团有限公司党组成员、副总经理,云南澜沧江水电开发有限公司党组书记、总经理、董事长,中国华能集团公司党组成员、副总经理,国家电网有限公司党组副书记、总经理、党组书记、董事长,中国大唐集团有限公司党组副书记、总经理、副部级领导干部等职务上的便利,以及职权、地位形成的便利条件,通过其他国家工作人员职务上的行为,为有关单位和个人在项目承揽、企业经营、职务晋升等事项上提供帮助,直接或通过他人非法收受上述单位和个人给予的财物,共计折合人民币1.54亿余元。(新华)

陈志犯罪集团核心骨干成员

李雄被押解回国

新华社电 记者从公安部获悉,4月1日,在柬埔寨有关部门大力支持下,公安部派出工作组,成功将陈志犯罪集团核心骨干成员李雄从柬埔寨金边押解回国。这是中柬执法合作取得的又一重大战果。

经查,李雄曾任太子集团旗下汇旺集团董事长,涉嫌开设赌场、诈骗、非法经营、掩饰隐瞒犯罪所得等多项犯罪。目前,李雄已被依法采取强制措施,相关案件正在进一步侦办中。

公安部有关负责人表示,陈志犯罪集团已有多名骨干成员陆续到案,公安机关将继续加大工作力度,坚决将在逃人员缉捕归案。同时再次正告犯罪分子,认清形势、悬崖勒马,尽早投案自首,争取宽大处理。