它山之石资料汇编

西安交通大学网络信息中心　　2026 年 3 月 12 日

一、国家与地方动态

1. 工信部发布关于防范 OpenClaw（“龙虾”）开源智能体安全风险建议

近日，工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）监测发现，开源 AI 智能体 OpenClaw 在默认或不当配置情况下存在较高安全风险，极易引发网络攻击、信息泄露等安全问题。3 月 11 日，NVDB 发布《关于防范 OpenClaw（“龙虾”）开源智能体安全风险的“六要六不要”建议》。2 月 5 日，NVDB 发布《关于防范 OpenClaw 开源 AI 智能体安全风险的预警提示》，并建议相关单位和用户在部署和应用 OpenClaw 时，充分核查公网暴露情况、权限配置及凭证管理情况，防范潜在网络安全风险。

网址链接：https://news.cctv.cn/2026/03/11/ARTIU9NPnXcPCDiU9cOfqT1D260311.shtml

二、高校动态

2. 北京大学：关于安全使用 OpenClaw 开源 AI 智能体的提醒

北京大学计算中心于 3 月 10 日发布了一则关于安全使用开源 AI 智能体 OpenClaw（又称“龙虾”）的重要提醒。

OpenClaw 是一款功能强大的 AI 助手工具，能访问本地文件、浏览器和邮件等，自 2025 年底推出后在全球范围内迅速流行，校内已有部分师生部署。然而，由于其默认配置存在严重安全隐患，若不加防护直接使用，极易引发信息安全问题。

主要风险包括：默认完全开放、无任何身份认证，导致暴露在网络上的实例可被任何人远程控制；存在高危漏洞，用户仅需点击一个恶意网页就可能被攻击者完全控制电脑；其第三方技能市场中发现大量恶意软件包，而 AI 默认可自动安装；此外，各类 API 密钥在配置文件中均为明文存储，一旦被入侵将直接泄露。

为保障安全，计算中心建议用户立即对照清单排查：务必检查并确保服务端口（18789）仅监听本地地址，绝不可暴露在公网；必须启用强身份认证；使用低权限专用账户运行；严格管理所有密钥；并避免在工具中存储任何敏感信息。校园网用户需特别注意，计算中心将定期扫描，发现未加固的实例会通知整改。网址链接：https://its.pku.edu.cn/announce/tz20260310195800.jsp

3. 中山大学：OpenClaw 智能体系统安全风险揭示及治理建议

OpenClaw 是典型的“执行型智能体”，由大模型驱动，能自动调用命令行、文件系统、浏览器等工具完成复杂任务。其核心风险从内容安全扩展为真实的系统级威胁，因为它拥有传统软件很少具备的“泛化执行权限”，可能导致文件泄露、主机被控，甚至成为攻击者跳板。CVE-2026-25253 等高危漏洞已被公开，且第三方评测显示其提示注入攻击成功率极高，风险已具备现实攻击条件。

其风险根源在于智能体无法可靠区分“指令”与“数据”。用户输入、网页、邮件等多源信息均以文本形式进入推理上下文，攻击者可将恶意提示嵌入其中，诱导模型误判为任务指令执行，

即间接提示注入。

主要安全风险包括：提示词注入，攻击者可隐藏指令改变智能体目标，如诱导其读取并外发配置文件；系统提示词泄露，攻击者可诱导输出内部规则后设计绕过策略；凭证泄露，如 CVE 漏洞可致认证 token 被窃，实现远程代码执行；工具调用越权，攻击者可组合使用文件读取、压缩、外发等合法工具链完成数据窃取，传统检测难以识别；多步任务链路失控，单步错误可能被放大，模型可能为完成任务跳过安全校验；记忆投毒，恶意规则可被写入长期记忆，在未来任务中自动触发形成“软后门”；供应链风险，恶意技能包或篡改的依赖库可引入后门。

典型攻击链包括：用户点击恶意链接即触发 Token 窃取与远程命令执行；网页隐藏指令诱导智能体读取系统文件并上传；多轮对话在记忆中植入后门规则，未来自动激活。

这些风险将导致严重的数据泄露、系统被远程控制、业务中断或配置篡改，以及因违规处理数据而引发的合规与法律风险。

治理必须从“模型对齐”升级为“系统安全工程”。核心策略包括：严格网络隔离，管理端口不暴露公网并启用来源校验；凭证加密存储、定期轮换并采用最小权限；工具权限最小化，高危工具默认关闭或强制人工审批；输入分层，严格区分用户指令与外部内容，后者不得作为可执行指令；记忆治理，防止存储敏感数据并支持审计清除；供应链治理，要求插件签名校验并锁定依赖版本。OpenClaw 应被视为高风险平台，在生产环境部署前

需建立持续评估机制。

网址链接：https://mp.weixin.qq.com/s/Cbx2RrBIG4P8jjrCHQ8CZA

4. 山东大学：使用 OpenClaw 等开源智能体安全提示

自 2025 年 AI 应用爆发后，2026 年 OpenClaw（“小龙虾”）作为任务执行式 AI 智能体火爆出圈，能协助用户管理邮件、操作浏览器、读写文件等，“养虾”热升温。但工信部 NVDB 平台监测发现，OpenClaw 在默认或不当配置下存在较高安全风险，因其“信任边界模糊”且能自主决策调用资源，易引发网络攻击和信息泄露。

为安全“养虾”，应在测试机或 Docker 沙箱部署，避免安装在主力或办公电脑，配置防火墙勿将网关端口（18789）暴露于互联网；创建普通用户启动服务，仅授予必需权限；尽量连接本地大模型确保“数据不出域”；并持续关注官方安全公告。

此外，师生使用 AI 普遍面临多重风险：向 AI 输入科研数据、个人信息可能被记录泄露；AI 生成虚假内容易导致学术失真和版权问题；不法分子利用 AI 模仿他人进行精准钓鱼诈骗；非官方渠道的 AI 工具可能植入恶意代码。防范关键在于不向 AI 输入核心数据与敏感信息，对生成内容交叉验证，通过官方渠道核实转账等要求，并从官方渠道下载应用及时更新。

网址链接：https://mp.weixin.qq.com/s/fmMD4mswiKf9Ne2ATYp61g

5. 华南师范大学：谨慎使用"龙虾"OpenClaw，这些安全风险要注意

开源 AI 智能体“龙虾”（OpenClaw）近期在校园内受到广泛关注，但其存在多项安全隐患。工业和信息化部、国家互联网应急中心等部门已发布相关安全风险提示。

OpenClaw 为实现“自主执行任务”，被授予了较高的系统权限，但其默认安全配置极为脆弱，攻击者一旦发现突破口即可轻易获取系统完全控制权。该工具存在权限边界模糊的问题，可能误解用户指令执行删除文件等有害操作；第三方技能包可能被植入恶意代码；即使更新到最新版本也无法完全消除风险；运行过程中还可能产生意料之外的高额 API 调用费用。

为保障校园网络安全，校园内严禁在生产环境和办公电脑安装 OpenClaw；严禁向其提供任何办公系统账号密码、科研数据等敏感信息；严禁开放公网访问。

如确需进行学习测试，必须严格遵守以下要求：在隔离的虚拟机环境中运行；严格控制端口访问权限；坚持最小权限原则，对关键操作进行二次确认；谨慎处理敏感信息；从官方渠道下载资源，仔细审查第三方技能包代码。

网址链接：https://mp.weixin.qq.com/s/ZFUULXwpCgzA2MGYgRUTvA

6. 华中师范大学：关于警惕开源 AI 智能体 OpenClaw（“龙虾”）安全风险的提醒

工业和信息化部网络安全威胁和漏洞信息共享平台监测发现，开源 AI 智能体 OpenClaw（“龙虾”）在默认或不当配置下存在较高安全风险，极易引发网络攻击和信息泄露。OpenClaw 可在本地私有化部署，具备持久记忆和主动执行能力，但其“信任边界模糊”，且能自主决策、调用系统资源。在缺乏有效权限控制和安全加固的情况下，可能因指令诱导、配置缺陷或被恶意接管，导致信息泄露、系统受控等后果。

为保障网络安全，信息化办公室提醒：立即核查校内是否存在 OpenClaw 部署，重点排查公网暴露情况、权限配置与凭证管理；如确需使用，应立即关闭不必要的公网访问，完善身份认证、访问控制、数据加密等机制，严格限制权限；密切关注官方安全公告及国家主管部门的加固建议，及时更新补丁；发现疑似安全事件请立即联系信息化办公室；严禁在信息化办公室分配的服务器上安装 OpenClaw。

网址链接：https://nisc.ccnu.edu.cn/info/1013/5889.htm

7. 西北工业大学：警惕“养龙虾”风险！高校师生必看的 OpenClaw 安全提示

近期，开源 AI 智能体 OpenClaw（“龙虾”）火爆出圈，它能根据指令自主规划并执行复杂任务，标志着 AI 正从“对话”迈向“执行”的新阶段。然而，工信部提醒，OpenClaw 在默认或不当配置下存在较高安

全风险，可能引发网络攻击和数据泄露。

单位或个人在部署使用前，需做好充分排查，重点关注公网暴露、权限配置及凭证管理，及时关闭不必要的公网访问入口；同时完善身份认证、访问控制、数据加密和安全审计等机制，并持续关注官方安全公告与加固建议，及时修复风险。

在日常使用中，务必不安装来源不明的第三方技能插件，防止恶意功能植入；严格遵循“最小权限”原则，不授予不必要的系统或 Root 权限，建议在隔离环境中运行；此外，OpenClaw 软件免费但其 API 调用可能产生费用，需合理规划避免资源超支。

技术热潮值得拥抱，但安全底线不能丢。在“养龙虾”的路上，务必系好安全带，防范潜在风险。

网址链接：https://mp.weixin.qq.com/s/0fqBI8gDJNQuIVJLylC0NA

8. 安徽师范大学：关于防范“龙虾”（OpenClaw）AI 智能体网络安全风险的预警通知

近期，开源 AI 智能体框架 OpenClaw（“龙虾”）因能自主执行电脑操作而走红，但已被工信部平台发布安全预警，存在极高安全风险。

其核心隐患包括：运行需获取电脑高权限，用户聊天记录、账号密码等均以明文存储，配置不当易被窃取；该工具存在意图误解问题，曾出现无视限制批量删除邮件、误删重要文件等失控案例；因其信任边界模糊且能自主调用系统资源，缺乏权限控制时易被恶意接管，导致电脑系统被远程控制；此外，该工具本质

是面向开发者的底层框架，普通用户若通过非官方“代装”服务部署，不仅可能因不懂配置放大风险，还可能遭遇投机骗局。

为此，全校师生应遵循非必要不部署的原则，切勿盲目跟风安装，尤其避免在办公电脑及存有敏感数据的设备上使用。严禁在处理教学科研数据、行政信息等工作场景中使用该工具。若确有技术研究需求，务必通过官方渠道获取资源，关闭不必要公网访问，完善身份认证与数据加密，并严格管理 API 密钥。切勿轻信网上“公益安装”等代装服务。已部署使用的师生应立即排查设备，核查公网暴露与权限配置，及时备份数据。一旦发现设备异常或信息泄露，须第一时间断网处置并向学校信息化办公室报告。

网址链接：https://imc.ahnu.edu.cn/info/1080/6752.htm