关于防范 OpenClaw 开源 AI 智能体网络安全风险及安全使用的提醒

近期，开源 AI 智能体 OpenClaw（因图标特征被俗称 “龙虾”，曾用名 Clawdbot、Moltbot）在网络上快速走红，该工具由奥地利程序员 Peter Steinberger 于 2025 年 11 月推出，可访问本地文件、浏览器、邮件等并自主执行电脑操作,因功能强大成为 GitHub 平台增长最快的开源项目之一，但该工具在默认或不当配置下存在极高安全风险，据国家信息安全漏洞库（CNNVD）统计，2026 年 1 月至 3 月 9 日已采集该工具漏洞 82 个，其中超危漏洞 12 个、高危漏洞 21 个。3 月 10 日，国家互联网应急中心正式发布风险警示，指出其存在提示词注入、插件投毒、权限失控等严重风险。

为切实保障我校师生个人信息安全、校园网络安全及教学科研数据资产安全，结合学校实际及国家相关部门监测信息，现就有关事宜提醒如下：

一、严守安全红线，合规安装和使用

1.全校教职工避免在学校办公电脑、服务器、教学终端、智能设备等各类生产环境设备上安装、运行 OpenClaw 软件本体、衍生版本及配套插件。避免在处理教学科研数据、行政办公信息、学生信息等工作场景中使用该工具。

2.确因学习、研究需要测试该工具功能的，必须在与校园网、办公系统完全隔离的测试机、Docker 沙箱或虚拟机中部署，严禁直接开放公网访问或输入任何敏感信息。

二、立即全面自查，消除安全隐患

即日起，已部署使用的是师生，对照以下清单进行全量安全排查与整改。

1. 排查公网暴露情况

检查 OpenClaw 的网关端口（18789）是否监听在公网可达的地址上，不同系统可运行对应命令核查：

Linux 用户：ss -tlnp | grep 18789

macOS 用户：lsof -i :18789

Windows 用户（PowerShell）：netstat -ano | findstr ":18789"

若输出显示 “0.0.0.0:18789” 或 “:::18789”，说明实例已暴露在所有网络接口上，请立即在 OpenClaw 的 “openclaw.json” 中修改为仅监听本地地址：

plaintext

```
{
    gateway: {
        mode: "local",
        port: 18789,
        bind: "loopback"
```

```
    }
}
```

2. 启用身份认证机制

OpenClaw 默认未启用网关认证，未认证实例一旦被网络访问，任何人均可远程连接操作。请务必开启认证并设置至少 32 位随机字符串作为认证令牌：

```
plaintext
{
    gateway: {
        mode: "local",
        port: 18789,
        bind: "loopback",
        auth: {
            token: "设置至少 32 位随机字符串",
        }
    }
}
```

3. 配置访问控制权限

遵循**最小权限原则**，为 OpenClaw 使用专用的低权限系统账户运行，切勿以 root 或管理员身份运行；限制其对文件系统、网络和系统资源的访问范围，在服务器部署的需配置防火墙，仅开放必要端口。

4. 规范凭证管理方式

OpenClaw 默认明文存储 API 密钥，被入侵后攻击者可直接获取。请及时检查凭证存储状态，若怀疑凭证已泄露，立即更换所有相关密钥和密码。

5. 加强敏感信息保护

切勿在 OpenClaw 中存储或处理任何敏感信息，包括银行卡信息、邮箱及社交媒体账号密码、科研涉密数据等。

三、清晰认知风险，严格规范操作

OpenClaw 因部署时 “信任边界模糊”，且具备自主决策、调用系统和外部资源的特性，缺乏有效安全控制时易引发各类安全问题，核心风险包括：

1. 默认缺失身份认证

出厂配置未开启任何身份验证，暴露在网络上的实例可被任何人远程访问，进而执行命令、读取文件、窃取各类凭据。

2. 远程代码执行漏洞

攻击者可通过恶意网页劫持用户本机的 OpenClaw 会话，用户仅需打开攻击页面，攻击者即可获得完整系统控制权限，利用门槛极低（参考 CVE-2026-25253）。

3. 易受技能供应链攻击

其技能市场 ClawHub 中曾发现 341 个恶意技能包，含键盘记录器、凭据窃取器等，约 36.82% 的技能存在可利用

安全缺陷，且默认配置下 AI 可自动安装技能，无需用户确认。

4. API 密钥明文存储

各类服务 API 密钥以明文形式保存在本地配置文件，实例被入侵后将直接泄露，易造成经济损失和信息泄露。

5. 端口暴露引发网络攻击

网关端口若未做限制暴露在公网或校园网，极易成为网络攻击切入点，引发系统被远程控制、数据被盗取等问题。

四、试用和探索建议

针对确需进行研究的合规使用场景，我们建议严格遵守以下安全操作规范。

1. 做好运行环境隔离

仅在隔离的测试机、沙箱或虚拟机中部署，与校园网、办公系统、个人敏感数据存储设备完全断开连接。

2. 强化网络访问管控

配置防火墙关闭不必要的端口映射，不将 OpenClaw 网关端口暴露于互联网或校园网，确需远程访问的，通过 SSH 等加密通道认证并严格限制访问源地址。

3. 坚持官方渠道获取

仅从 OpenClaw 官方渠道下载最新稳定版本，开启自动更新提醒，升级前做好数据备份，切勿使用第三方镜像版本、历史版本及非官方 “代装” 服务。

4. 审慎使用第三方技能

不随意下载 ClawHub 技能包，安装前务必核查代码内容，拒绝使用要求 “下载 ZIP 压缩包”“执行 shell 脚本” 或 “输入密码” 的技能包，防止恶意代码植入。

5. 加强设备安全监控

定期检查部署设备是否存在异常进程、陌生网络连接，及时更改相关账号密码；设置文件与 Http 访问白名单，明确约束模型不得将外部内容视为可执行指令，做到 “数据不出域”。

6. 警惕钓鱼攻击风险

部分漏洞利用仅需打开恶意链接，使用 OpenClaw 期间，对来源不明的链接、文件、二维码务必保持警惕，不随意点击访问。

五、安全相关参考资源

为帮助大家更规范地开展安全配置、加固及问题排查，整理以下官方及专业安全资源，可供参考学习。

1. OpenClaw 官方安全文档：

https://docs.openclaw.ai/gateway/security

2. CVE-2026-25253 漏洞详情：

https://nvd.nist.gov/vuln/detail/CVE-2026-25253

3. OpenClaw 官方加固指南：

https://github.com/openclaw/openclaw/discussions/12606

4. SlowMist 安全验证指南：

https://github.com/slowmist/openclaw-security-practice-guide

5. Microsoft 安全部署建议：

https://www.microsoft.com/en-us/security/blog/2026/02/19/running-openclaw-safely-identity-isolation-runtime-risk/

如发现校园网络异常、疑似安全攻击行为，或在 OpenClaw 安全排查、配置过程中遇到问题，请及时联系学校数字信息中心。电话：63393609，联系邮箱：nynzxxzx@163.com。

数字信息中心

2026 年 3 月 12 日