新聞剪影

「龍蝦」安全風險引發全球警覺，中國發佈安全使用指南

【俄羅斯衛星通訊社3月23日電】隨著開源人工智能體OpenClaw（龍蝦）在全球科技圈的迅速走紅，其暴露出的系統性安全風險已引發多國監管機構的高度警惕。

3月22日，中國國家互聯網應急中心、中國網絡空間安全協會聯合發佈《OpenClaw安全使用實踐指南》，面向普通用戶、企業用戶、雲服務商以及技術開發者等，提出安全防護建議。

OpenClaw憑藉強大的自然語言交互與任務執行能力迅速走紅。作為可自主執行現實任務、代表用戶行動的智能體，它標誌著人工智能從「對話助手」向「行動助手」的跨越。然而，其開放性與高權限特性也帶來多重安全隱患：

第三方技能包或依賴庫可能被惡意篡改，用於竊取核心數據或控制系統；

開發運行時所需的高權限若配置疏漏，易導致主機敏感信息洩露甚至被劫持發起網絡攻擊；

在處理通訊錄、日程、聊天記錄等個人信息時，也存在數據被竊取與濫用的風險。

這些安全隱患已引發全球性警覺。3月8日，中國工業和信息化部網絡安全威脅和漏洞信息共享平台發佈預警提示，監測發現OpenClaw部分實例在默認或不當配置情況下存在較高安全風險。美國、歐盟、英國、日本、韓國等多國監管機構也相繼發出警示，部分大型企業及金融機構已緊急禁止辦公設備安裝OpenClaw。

在此背景下，中國發佈的安全使用實踐指南為不同用戶群體提供了清晰的操作指引：

對於普通用戶，指南建議使用專用設備、虛擬機或容器安裝OpenClaw並做好環境隔離，不宜在日常辦公電腦上安裝；不使用管理員或超級用戶權限運行；不在OpenClaw環境中存儲、處理隱私數據；及時更新最新版本。

對於雲服務商，指南建議做好雲主機基礎安全層面的安全評測與加固，做好安全防護能力部署、接入，做好供應鏈及數據安全防護。

目前，聯合國、國際標準化組織等國際機構正積極推進行動型AI安全標準與監管框架的建立，各國也在加強安全協作。從技術爆紅到風險預警，OpenClaw引發的全球關注深刻詮釋了人工智能進入行動時代的機遇與挑戰，安全已成為這一領域創新發展的前提與基石。

ISSN 1018-107-5
00004
9 771018 107005
中華郵政北台字第3737號執照登記為雜誌交寄

海峽評論

1991年1月1日創刊　創辦人 王曉波　2026年04月出版・424期

兩岸通商通郵通航後要通電通氣

↑航行中的USA巨輪陷伊朗戰火，濃煙滾滾上升，象徵美國聯邦預算在以「每天10億美元」化為煙霧。（原載美國卡格爾漫畫網站）