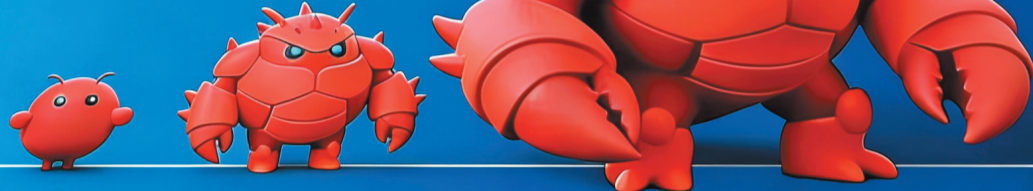


OpenClaw版本升级“翻车”

近日爆火的智能体“龙虾”OpenClaw在一场史上最大版本的更新后，因激进、无兼容层的破坏性重构，导致大量用户反馈插件瘫痪、功能失效，成为OpenClaw诞生以来最严重的一次升级事故。与此同时，经过全民“养虾”热潮之后，隐忧渐显。OpenClaw的强大源于让渡权限带来的操作空间，一旦错误理解指令或者遭遇攻击，不仅可能误删核心数据，更可能沦为黑客潜入内网的跳板。

OpenClaw相关“升级事故”



- 流量瞬间暴增，导致新版本全线报错，具体包括dist/control-ui目录缺失、插件系统崩溃等问题
- 运行阶段微信、飞书等通讯插件无法加载、直接瘫痪
- 微信ClawBot插件更新后完全无法同步消息
- 浏览器扩展Relay功能因路径移除而失效，MiniMax等国产品模型配置异常，Windows沙箱出现权限错误

升级事故

当地时间3月23日，OpenClaw迎来诞生以来最大规模更新，包括插件系统彻底重构、模型升级、安全加固、沙箱架构升级、生态整合等方面。

新版本定位为跨平台的个人AI助手，更新重点涉及底层架构调整，包括OpenClaw插件安装优先从ClawHub(OpenClaw官方专属插件市场)安装，而非npm(标准Node.js官方包管理器)；删除旧插件系统，使用全新的插件开发工具包。

npm是全球JavaScript开发者共用的公共基础设施，可以免费下载、上传代码插件，成为全球程序员可以共享代码模块的公共仓库。但该特点也伴随着恶意插件随便上传、无

法审核或管控、极易被投毒等问题。这也是此次OpenClaw放弃npm、转用ClawHub的重要原因。

然而，这场以“安全与生态统一”为目标的激进重构，却直接演变成一次严重的“升级事故”。由于OpenClaw此次强行将插件生态从公共npm迁移到官方ClawHub，引发流量瞬间暴增，导致新版本全线报错，具体包括dist/control-ui目录缺失、插件系统崩溃等问题。

国内平台也受到不少影响。例如运行阶段微信、飞书等通讯插件无法加载、直接瘫痪，部分用户反馈微信ClawBot插件更新后完全无法同步消息；浏览器扩展Relay功能因路径移除而失效，MiniMax等国产品模型配置异常，Windows沙箱出现权限错误。

有开发者反馈称：这是一次糟糕的更新，

所有插件技能都必须上传至ClawHub才能用，之前常用的很多插件未同步至ClawHub，且请求次数增加后会发生速率限制。另一位开发者表示，新版本会导致WhatsApp插件失效，升级后频道停止了服务，需要回滚处理。

针对ClawHub访问异常问题，OpenClaw开发者彼得·斯坦伯格(Peter Steinberger)回应称：为了抵御频繁的网络攻击，限流规则设置得过于严格。后续会调整限流策略，放宽限制以恢复正常访问。

这也揭开了本次升级“翻车”的原因：大量用户在升级后涌入ClawHub寻找新插件，修复旧插件问题，叠加可能的恶意流量攻击，触发了ClawHub的限流机制，进一步加剧了用户体验的崩溃：旧插件无法用，新插件下不了。

“极客玩具”

将时间线拉回几个月前，OpenClaw凭借“让AI操控电脑”的核心能力，成为开源社区的现象级项目。它的GitHub星标数逆势飙升，开发者们争相“领养龙虾”，用一句话指挥AI完成从打开应用、浏览网页到填写表格的一切任务。

互联网从业人士从慧对北京商报记者表示，OpenClaw的魅力在于它的开放性。作为一个开源框架，它允许开发者自由配置模型、自定义插件，甚至可以接入各种大模型——从GPT-5.4到MiniMax M2.7，从Claude到GLM。这种灵活性让技术极客们如获至宝，他们用OpenClaw搭建各种自动化工作流，在社交媒体上分享自己的“龙虾饲养心得”。

在另一位AI算法工程师华丰看来，OpenClaw的爆火是一个清晰的信号：AI正在从“能说会道”的聊天伙伴，转向“能动手做事”的执行实体。“真正能落地、干活的AI，才是对人有用的AI。从这个意义上说，智能体是技术发展的必然方向。”

“但OpenClaw有一个致命的门槛：它需要用户自行部署、调试、配置。”从慧坦言，当前AI智能体普遍面临“部署繁琐、配置复杂、执行不稳定”的问题，普通用户常常被环境搭建、参数调试、权限管理等技术环节挡在门外。这意味着，OpenClaw本质上是一个“极客玩具”，而非大众工具。

华丰也表示，媒体的广泛传播制造了一种“不用即落后”的焦虑，目前市场上还没有出现真正成熟、开箱即用的商业化产品。当前的这类工具，本质上更多是面向开发者、程序员群体。

爆火之后

此次OpenClaw升级的同时，行业对“龙虾系列”的安全问题愈发关注。3月22日，国家

互联网应急中心、中国网络空间安全协会联合发布OpenClaw安全使用实践指南，面向普通用户、企业用户、云服务商以及技术开发人员等，提出安全防护建议。

从个人隐私泄露到关键基础设施瘫痪，已经有受害者付出惨痛代价。OpenClaw工程师测试时，其创建的交易智能体因被虚假求助话术诱导，本应转账4美元，却误将价值25万美元的加密货币全部转出；Meta公司AI安全总监让“龙虾”整理邮箱并标注“未经批准不得操作”，结果AI因上下文窗口被占满，无视安全指令疯狂删除邮件，最终只能靠物理手段终止程序；更有用户因让OpenClaw操作生产环境，导致平台两年半的194万行数据被彻底清空。

邢金董首席经济学家邢星表示，OpenClaw可能带来的核心风险集中在数据安全、交易可控性及合规性三个层面，其开源属性导致的安全漏洞的易利用性，会放大风险传导效应。这些风险的凸显，本质是由金融行业的核心特点决定的。金融行业承载着海量敏感信息，对数据保密性、完整性要求极高，且行业具有强关联性，单个环节的风险易扩散为系统性风险；同时，金融交易的严肃性和不可逆性，以及监管对合规性的零容错要求，使得开源AI智能体的弱安全配置和责任界定模糊问题，与行业特性形成天然矛盾。

隐私泄露规模更为惊人。截至目前，全球已有超27万个OpenClaw实例直接暴露于公网，处于零认证“裸奔”状态。更可怕的是，ClawHub技能市场中约12%的插件被植入恶意代码，可窃取用户的SSH密钥和浏览器密码。

邢星指出，整体来看，OpenClaw新版本是一个以开发者与安全性为导向的版本，但在安全性、可用性与用户体验之间的失衡，说明面向用户的生态迁移与工程化落地仍需更细致的打磨，激进的架构调整需搭配充分的兼容预案、流量测试与用户过渡方案。

北京商报记者 赵天舒

聚焦 Focus

马斯克自建全球最大芯片厂

美国当地时间3月21日，特斯拉宣布将与SpaceX、xAI合作建设芯片项目TeraFab，目标是实现年产能1太瓦(1万亿瓦)AI算力，打造全球规模最大的芯片制造工厂。据特斯拉披露，TeraFab将是一座垂直整合的芯片工厂，涵盖芯片设计、推理和存储芯片制造、封装与测试全流程，并配备所有必要设备，用于测试、修改和制造芯片。

在发布会上，特斯拉CEO马斯克称，现在地球上所有芯片晶圆厂的产能总和约为20吉瓦(1吉瓦=0.001太瓦)，仅相当于其所需算力的2%左右。马斯克在发言中强调了对现有供应链的依赖，也表达了对第三方扩产速度的无奈。他透露，自己曾向三星、台积电和美光等供应商承诺，会买下它们所能生产的所有芯片，“但他们扩张产能的速度远低于我们的期望”。

TeraFab的核心亮点在于其工艺整合模式。根据马斯克描述，位于美国德州奥斯汀的先进制程工厂将集成光刻掩模制作、逻辑芯片生产、存储芯片生产、封装以及测试等全套流程，实现“芯片设计、流片、测试、改版掩模、再流片”的快速迭代。所有环节都在同一工厂内反复进行，以极快速度改进芯片设计。

按照规划，TeraFab瞄准2纳米先进制程，将主要聚焦两类芯片的量产：一类是主要用于特斯拉汽车及Optimus人形机器人的芯片，针对边缘计算和推理优化，包括特斯拉正在研发的AI5和下一代芯片AI6。另一类则是专为太空环境与低轨AI卫星打造的太空算力芯片，首款产品命名为D3。此类芯片针对太空辐射环境进行了专门防护设计，并在热管理策略上有别于地

面产品，通过适度提高运行温度以减轻散热器重量。

TeraFab规划年产能1000亿至2000亿颗AI级存储芯片，相当于每月约10万片晶圆投片量。首批量产芯片为AI5，计划于2027年投产，用于全自动驾驶、人形机器人Optimus、无人出租车Cybercab及数据中心。

马斯克还指出，由于在地球上建设大规模数据中心面临电力限制，只有在太空中充分利用太阳能才能实现更大规模计算。TeraFab的芯片产能中，将有20%用于特斯拉汽车和Optimus机器人，剩余80%将用于在太空搭建超大规模计算集群，“太空将代表绝大多数算力”。

马斯克在发布会上首次展示了一个概念性太空AI计算卫星，功率约为100千瓦，配备太阳能电池板和散热器，未来可达到兆瓦级别。他还设想在月球建设发射基地，进一步将太空算力规模提升至1拍瓦，即1太瓦的1000倍。

为实现该计划，马斯克估算需要将约1000万吨物资送入轨道。SpaceX正推进Starship V3版本的运力升级，将单次载荷从100吨提升至200吨；Starship V4将进一步提升载荷能力。

马斯克表示，TeraFab最终将协助人类成为能够利用其他行星与恒星资源的“银河文明”，但他未公布TeraFab量产的具体时间表。

然而，业界对TeraFab项目的可行性仍持保留态度。半导体制造涉及数百亿美元规模投资、极紫外光(EUV)光刻机供应以及专业人才。英伟达CEO黄仁勋曾指出，建设先进芯片制造工厂极其困难，这不只是建厂房的问题，芯片工厂需要数十年的工程、科学与技术经验积累。此外，先进制程高度依赖EUV光刻机，而该设备供应商集中、交期长且成本昂贵，并非单靠资金即可快速取得。

资金方面，有业内人士表示，建造一座采用2纳米先进制程的晶圆厂，通常需要250亿美元至400亿美元投资，建设周期长达3至5年。这对于特斯拉当前的财务状况构成了巨大压力。马斯克并未透露TeraFab的初期投资金额，此前有消息称，该数字介于200亿美元至250亿美元之间。

摩根士丹利分析师Andrew Per-coco将TeraFab项目称为一项“艰巨的任务”。他估算，该设施的全部成本可能会飙升至350亿美元至400亿美元。该分析师进一步警告称，即使在乐观的情境下，该工厂在2028年之前也无法实际生产出芯片。

另一家投行Wedbush的分析师Dan Ives称，TeraFab项目应由特斯拉主导，并与潜在芯片伙伴合作推进的项目。他认为，打造太空算力集群是明智的AI战略，但独立建造芯片工厂的成本与周期不可控。

北京商报综合报道

· 图片新闻 ·

霍尔木兹海峡通航量暴跌逾九成



波斯湾地区紧张局势升级后，霍尔木兹海峡海上航运量明显下降。视觉中国/图

自美以冲突爆发以来，全球能源运输“命门”霍尔木兹海峡航运严重受阻。市场服务机构数据显示，3月以来，商船通过这一海峡的次数较冲突前下降了95%。

法新社23日援引市场服务机构克普勒公司数据报道，自3月1日至格林尼治时间3月23日16时，商船通过霍尔木兹海峡的次数仅为144次，较2月28日冲突爆发前减少95%。其中91次通航为运输石油和天然气的船只，多数驶离海峡向东航行。

由美国海军主导的多国机构“联合海上信息中心”数据显示，冲突前每天约有138艘船只通过该海峡。

法新社说，23日通过霍尔木兹海峡的船只似乎都使用了一条北部航线。据称，该航线位于伊朗拉穆克岛以北，由伊朗政府批准。

英国《劳埃德船舶日报》23日报道，“霍尔木兹海峡的航运持续受到严重干扰”，当天已追踪

到超过20艘船只使用了这条航线。该日报此前说，这条航线类似于伊朗伊斯兰革命卫队划定的“安全走廊”。伊斯兰革命卫队利用拉穆克岛监视确认通过海峡的船只。

国际货运信息平台上海上交网站数据显示，在供应受限的情况下，自3月3日以来，约有11艘原本前往欧洲的液化天然气运输船已改道驶向距离更近、现货价格更高的亚洲。

摩根大通的分析师表示，通过霍尔木兹海峡的可观测石油运输中，伊朗石油占比高达98%，3月初运输量为日均130万桶。

霍尔木兹海峡是全球石油运输的重要海上要道。作为波斯湾通往外部的唯一航道，全球海运石油贸易总量的逾四分之一、全球液化天然气运输量的约五分之一经由该海峡运往世界各地。美国能源信息局估计，2024年经过该海峡运送的油品数量日均约2000万桶。

北京商报综合报道