工业智能每日观察

中国高技术产业发展促进会新质生产力工作委员会

博雅云创 & 中科创新驱动

2026 年 5 月 3 日

摘要

Anthropic 发布 Project Glasswing 联合 12 家科技巨头保护关键基础设施，Claude Mythos 模型发现数千高危漏洞，对工业控制系统安全敲响警钟。Qualcomm 在 Investor Day 2026 宣布工业 AI 和物理 AI 战略。Merics 发布报告分析中国具身智能机器人产业雄心，深圳发布"AI+ 先进制造业" 行动计划。AI 辅助安全扫描发现存在 9 年的 Linux 内核漏洞，工业 Linux 系统面临紧急补丁需求。

Contents

1 Anthropic Project Glasswing：AI 网络安全能力跃升对工业基础设施的警示

1.1 Claude Mythos 发现数千高危漏洞，工业控制系统安全面临新挑战

据 Anthropic 官方博客 5 月 2 日发布，Project Glasswing 计划的核心发现是：AI 模型在发现和利用软件漏洞方面的能力已超越绝大多数人类安全专家。Claude Mythos Preview 已在每个主要操作系统和网络浏览器中发现高危漏洞，其中一些漏洞在数十年的人工审查中从未被发现。对工业界而言，这一能力跃升意味着工业控制系统（ICS）、SCADA 系统和运营技术（OT）网络面临前所未有的安全威胁。Anthropic 在声明中明确提到，网络攻击已对企业网络、医疗系统、能源基础设施和交通枢纽造成严重后果，全球网络犯罪年度成本估计约 5000 亿美元。Project Glasswing 的 12 家合作伙伴中，Cisco、CrowdStrike 和 Palo Alto Networks 均是工

业网络安全领域的核心供应商。

1.2 漏洞发现到利用时间缩短至 10 小时，工业安全响应窗口急剧收窄

据 NeuralBuddies 报道，在 Black Hat Asia 2026 上，RunSybil CEO Ari Herbert-Voss 披露：从漏洞发现到可用利用代码的时间窗口已从 2023 年的五个月缩短至 2026 年的十小时。这对工业环境的影响尤为严峻——工业控制系统的补丁周期通常以周甚至月计算，远长于 IT 系统。当攻击者可以在 10 小时内将漏洞武器化时，工业企业的安全响应窗口已几乎不存在。Anthropic 承诺为 Project Glasswing 投入最高 1 亿美元的使用信用额度，并向开源安全组织直接捐赠 400 万美元。

2 Qualcomm Investor Day 2026：工业 AI 与物理 AI 成下一阶段增长核心

2.1 布局千兆瓦级数据中心、工业 AI 和 6G

据 WebWire 5 月 1 日报道，Qualcomm 在 Investor Day 2026 上由总裁兼 CEO Cristiano Amon 及高管团队阐述了公司下一阶段的增长和多元化战略。Qualcomm 将重点布局四大方向：千兆瓦级 AI 数据中心、工业 AI 与物理 AI 的快速发展、面向智能体工作负载的个人 AI，以及作为下一代无线技术的 6G。Qualcomm 高管特别强调，随着智能体工作负载（Agentic Workloads）驱动新一轮平台变革，Qualcomm 正在抓住 AI 在数据中心、工业现场和个人设备三个层面创造的机遇。工业 AI 和物理 AI 被明确列为公司战略重点，与 Nvidia 在汉诺威工博会上推广的 Physical AI 理念形成呼应，表明工业 AI 正从概念走向芯片级的产业化支撑。

3 Merics 报告：中国具身智能机器人产业的雄心路径

3.1 深圳发布”AI+ 先进制造业” 行动计划，政策驱动产业加速

据欧洲智库 Merics 5 月 2 日发布的深度研究报告，中国正通过雄心勃勃的政策路径推动具身智能（Embodied AI）机器人产业转型。报告引用了深圳市 2026 年 2 月发布的《深圳市” 人工智能 +” 先进制造业行动计划（2026-2027 年)》，以及工信部 2025 年发布的《场景化、图谱化推进重点行业数字化转型参考指引》，表明中国正在从中央到地方构建系统性的 AI+ 制造业政策框架。报告分析了中国在人形机器人、四足机器人和工业协作机器人领域的技术进展和产业化路径，指出中国企业正在从实验室研发快速走向商业化部署。报告认为，中国在具身智能领域的政策力度和产业投入正在形成与美国和欧洲不同的发展模式——更强调政府引导和场景驱动。

4 AI 辅助发现 9 年 Linux 内核漏洞，工业 Linux 系统面临紧急补丁

4.1 CVE-2026-31431 可导致 root 权限获取，影响所有主流发行版

据 Dark Reading 5 月 2 日报道，安全公司 Xint 的研究人员利用 AI 辅助代码扫描技术，在不到一小时内发现了一个存在 9 年之久的 Linux 内核漏洞。该漏洞被命名为”Copy Fail”（CVE-2026-31431），影响自 2017 年以来的所有 Linux 构建版本，可被利用获取 root 权限。这一发现对工业界具有直接影响：Linux 是工业控制系统、嵌入式设备、边缘计算网关和云端工业平台的主流操作系统。大量工业 Linux 部署运行的是长期支持（LTS）版本，补丁更新周期较长，且许多嵌入式工业设备难以远程更新。工业企业应立即评估其 Linux 系统版本并制定补丁计划。

5 参考文献

1. Anthropic (2026-05-02), *Project Glasswing: Securing critical software for the AI era*
2. NeuralBuddies (2026-05-01), *AI News Recap: Bug discovery to exploit collapsed from 5 months to 10 hours*
3. WebWire (2026-05-01), *Qualcomm to Outline Next Phase of Growth and Diversification at Investor Day 2026*
4. Merics (2026-05-02), *Embodied AI: China's ambitious path to transform its robotics industry*
5. 科技日报 (2026-02-13), 深圳市”人工智能 +”先进制造业行动计划 (*2026-2027* 年)
6. Dark Reading (2026-05-02), *Another AI-Assisted Software Scan Yields 9-Year-Old Linux Bug*
7. The Hacker News (2026-05-01), *New Linux 'Copy Fail' Vulnerability Enables Root Access on Major Distributions*
8. The Hacker News (2026-05-02), *Researchers Discover Critical GitHub CVE-2026-3854 RCE Flaw*
9. Digital Journal (2026-05-02), *Majority of cyberattacks are now driven by AI*
10. Forbes (2026-05-02), *AI safeguards can be averted—siloed cybersecurity creates dangerous blind spots*

联系我们，请扫描二维码

新质生产力工作委员会
官方公众号

工业智能算网
gyznsw.cn

新质生产力工作委员会：

中国高技术产业发展促进会新质生产力工作委员会，专注于推动工业人工智能、智能制造、数字化转型等前沿技术发展，为企业提供政策解读、技术咨询和产业对接服务。

工业智能算网：

专注于工业人工智能、新质生产力、工业软件 CAE、智能制造等前沿技术。提供每日动态分析、技术趋势解读、解决方案分享，推动工业智能化转型。

网站地址： https://gyznsw.cn