EINPRESSWIRE

Coalition for Secure AI Releases Extensive Taxonomy for Model Context Protocol Security

Collaborative Industry Effort Delivers Identity Management, Supply Chain Integrity, and Protocol Security for AI Agent Deployments

BOSTON, MA, UNITED STATES, January 27, 2026 /EINPresswire.com/ -- OASIS Open, the international open source and standards consortium, announced the release of the "Model Context Protocol (MCP) Security" white paper from the Coalition for Secure AI (CoSAI), an OASIS Open Project. This framework equips security professionals and developers to identify, assess, and mitigate risks in MCP-based AI agents, addressing the urgent need for standardized security practices as AI increasingly connects to external tools and services.

Securing the Bridge Between AI and the Real World

MCP, developed by Anthropic, a CoSAI Sponsor, together with a growing open source community, has emerged as a leading protocol for connecting AI agents to external tools, databases, APIs, and services. However, like any integration protocol, MCP deployments face active and evolving threats.

This security framework presents a well-defined taxonomy of nearly forty threats and concrete mitigation strategies across twelve distinct categories, spanning identity and access control, input validation, data protection, network security, supply chain integrity, and operational visibility. The framework distinguishes between traditional security concerns amplified by AI mediation and novel attack vectors unique to LLM-tool interactions, enabling security teams to implement defense-in-depth strategies tailored to their specific deployment patterns.

"As AI moves beyond chat models to agents, gaining the ability to take actions and interact with their environments and the real world through tool calling, the security implications and potential consequences are much more severe," said Ian Molloy, IBM, and Sarah Novotny, CoSAI's Workstream 4 Co-Leads. "This framework represents the expertise of CoSAI's members and contributors who understand that protecting agentic systems requires addressing everything from protocol-level authentication and supply chain integrity to guardrails, systems security and enforcement."

Collaborative Industry Effort

The MCP Security paper was developed by CoSAI's Workstream 4: Secure Design Patterns for Agentic Systems, drawing on contributions across CoSAI's Sponsors and partner organizations, including Premier Sponsors EY, Google, IBM, Meta, Microsoft, NVIDIA, PayPal, Snyk, Trend Micro, and Zscaler. Additional CoSAI AI Security Guidance Publications can be found on GitHub (https://github.com/cosai-oasis/).

Technical contributors, researchers, and organizations are welcome to participate in CoSAI's open source community and support its ongoing work. OASIS welcomes additional sponsorship support from companies involved in AI security. Contact join@oasis-open.org for more information.

About CoSAI

The Coalition for Secure AI (CoSAI) is a global, multi-stakeholder initiative dedicated to advancing the security of AI systems. CoSAI brings together experts from industry, government, and academia to develop practical guidance, promote secure-by-design practices, and close critical gaps in AI system defense. Through its workstreams and open collaboration model, CoSAI supports the responsible development and deployment of AI technologies worldwide. CoSAI operates under OASIS Open, an international standards and open-source consortium. www.coalitionforsecureai.org

About OASIS Open

One of the most respected, nonprofit open source and open standards bodies in the world, OASIS advances the fair, transparent development of open source software and standards through the power of global collaboration and community. OASIS is the home for worldwide standards in AI, emergency management, identity, IoT, cybersecurity, blockchain, privacy, cryptography, cloud computing, urban mobility, and other content technologies. Many OASIS standards go on to be ratified by de jure bodies and referenced in international policies and government procurement. www.oasis-open.org

Media Inquiries: communications@oasis-open.org

Mary Beth Minto
OASIS Open
+1 781-569-5113
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/886568779