EINPRESSWIRE

PointGuard AI Launches AI Security Incident Tracker for Agentic Threats

New public resource documents real-world AI, agentic, and MCP security incidents with structured risk scoring and expert analysis.

SAN JOSE, CA, CA, UNITED STATES, February 18, 2026 /EINPresswire.com/ -- PointGuard AI today announced the launch of its AI Security Incident Tracker, a public resource developed by the PointGuard AI Research Lab to monitor, document, and analyze major AI-related security incidents affecting enterprises, technology providers, and critical AI infrastructure.

> “
> There’s a lot of noise around AI security, but few resources that consistently track and compare incidents. We built this tracker to bring clarity and context to real-world AI threats.”
>
> *Pravin Kothari, CEO of PointGuard AI*

As AI adoption accelerates across enterprise applications, attackers are exploiting a rapidly expanding attack surface. Agentic AI, autonomous agents, and orchestration layers such as MCP are significantly increasing security exposure by introducing new tools, permissions, and dynamic execution paths.

“There’s a lot of noise around AI security, but few resources that consistently track and compare incidents using a structured methodology,” said Pravin Kothari, CEO of PointGuard AI. “We built this tracker to bring clarity and context to real-world AI threats.”

The PointGuard AI Research Lab collaborates with enterprise CISOs, security practitioners, industry experts, and technology partners to validate incidents and refine its methodology. The tracker focuses strictly on documented incidents and demonstrated vulnerabilities, supported by credible third-party sources such as NVD, MIT AI Risk Initiative, Cornell arXiv, GitHub, and the AI Incident Database.

To date, the Lab has documented nearly 80 significant AI-related security incidents across 2025 and 2026, with more than half occurring in the first 90 days of 2026. Incidents span major platforms including OpenClaw/Moltbook, Anthropic Claude, Microsoft Copilot, Google Gemini, ServiceNow, and Salesforce.

For each incident, there is analysis of what happened, how the breach unfolded, and mitigation guidance, with explainer videos for major cases. The tracker covers emerging risks including prompt injection, MCP and agentic vulnerabilities, AI coding and framework flaws, supply chain exposure, data leaks, credential theft, and model compromise.

To enable consistent comparison, the Lab introduced the AI Security Severity Index (AISSI), a 0–10 scoring system based on weighted factors including Criticality, Propagation, Exploitability, Supply Chain, and Business Impact.

“Agentic AI is rapidly expanding the attack surface,” said Kothari. “We designed this tool to help enterprises stay ahead of real incidents and protect their AI systems with confidence.”

The PointGuard AI Research Lab welcomes suggestions for incidents to include and feedback on methodology. To explore the tracker, and subscribe for updates visit:
https://www.pointguardai.com/ai-security-incident-tracker

Willy Leichter
PointGuard AI
email us here
Visit us on social media:
LinkedIn
YouTube