AI server compromised

The flaws, located in the Python backend component of Triton, can be exploited by remote, unauthenticated attackers to take complete control of affected AI servers, enabling remote ...

Analyze 6 major AI security incidents from April 2026. Get detailed attack paths on AI agent data leaks, global malware campaigns, and model exploitation.

A cyber attack hit LiteLLM, an open-source library used in many AI systems, carrying malicious code that stole credentials such as environment variables, SSH keys, and passwords.

In Jalisco alone, 37 database servers were compromised, including health records and domestic violence victim data. How it worked: the attacker told Claude he was running a legitimate ...

Security researchers at GitGuardian have uncovered a critical path traversal vulnerability in Smithery.ai, a popular Model Context Protocol (MCP) server hosting platform, that exposed over ...

A critical vulnerability in Smithery.ai, a popular registry for Model Context Protocol (MCP) servers. This issue could have allowed attackers to steal from over 3,000 AI servers and take API ...

A community-driven database of AI-related security incidents, data breaches, and leaks. Track and discover the latest AI security vulnerabilities.

Adversaries injected malicious prompts into legitimate AI tools at more than 90 organizations in 2025, stealing credentials and cryptocurrency. Every one of those compromised ...

Hackers are exploiting a critical vulnerability in Ray, an open-source AI framework, to launch widespread cryptojacking campaigns targeting exposed servers and high-value GPUs, ...

A compromised Context AI employee credential cascaded through an "Allow All" OAuth grant into Vercel, exposing environment variables and customer credentials now listed for sale on ...

AI server compromised

Web: https://tlaletsoglobal.co.za