AI Server Attack

Artificial intelligence (AI) is the capability of computational systems to perform tasks typically associated with human intelligence, such as learning, reasoning, problem-solving, perception, and decision ...

Security researchers have identified over 91,000 attack sessions targeting AI infrastructure between October 2025 and January 2026, exposing systematic campaigns against large language ...

This research demonstrates that MCP servers, both locally hosted and third-party, remotely hosted, introduce significant attack vectors that can be exploited to execute arbitrary code, ...

artificial intelligence (AI), the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings.

We believe our research will eventually lead to artificial general intelligence, a system that can solve human-level problems. Building safe and beneficial AGI is our mission.

Learn what artificial intelligence (AI) is and how it works, explore the different types of AI, see examples of AI, and discover the benefits of AI.

Artificial Intelligence (AI) is a term coined in 1955 by John McCarthy, Stanford"s first faculty member in AI, who described it as "the science and engineering of making intelligent machines." Today it is a ...

MCP design flaw enables RCE across 7,000+ servers and 150M downloads, impacting AI SDKs and supply chains.

Three architectural choices, common to most AI inference servers, drive these patterns and explain why fixes in one framework do not automatically protect users of another.

Hackers use AI to generate attack code targeting AI infrastructure, and then getting compromised AI systems to find others to attack, researchers warn in a new report.

For those unfamiliar with computer science, it can be overwhelming to try and grasp the many facets of artificial intelligence and their implications. Here, we break down what artificial intelligence is, how it ...

Meet Gemini, Google"s AI assistant. Get help with writing, planning, brainstorming, and more. Experience the power of generative AI.

As detailed in the report, Trend has found 200+ ChromaDB servers, 2,000 Redis servers, and 10,000+ Ollama

servers exposed to the internet with no authentication. Many AI frameworks and ...

Anthropic design choice Exposes 150M+ Downloads and up to 200K Servers to complete takeover The OX Security Research team has uncovered a critical, systemic vulnerability at the core ...

In this McKinsey Explainer, we define what AI is, and look at how rapid advances in Artificial Intelligence are reshaping almost every aspect of global society.

A security report has tightened the nerves within the AI development community. On April 15, the cybersecurity company OX Security released a report revealing a design flaw in Anthropic"s ...

Web: https://www.safireschools.co.za