AI attacked by malicious server



Overview

A popular Model Context Protocol (MCP) server used to deploy AI agents has turned malicious in one of its latest updates, according to Koi Security.

Article Content

The Real-World Attacks Behind OWASP Agentic AI Top 10

OWASP''s new Agentic AI Top 10 highlights real-world attacks already targeting autonomous AI systems, from goal hijacking to malicious MCP

Malicious AI Agent Server Reportedly Steals Emails

A popular Model Context Protocol (MCP) server used to deploy AI agents has turned malicious in one of its latest updates, according to Koi Security.

Adversarial Misuse of Generative AI

As part of that effort, we investigate activity associated with threat actors to protect against malicious activity, including the misuse of generative AI or LLMs. This report shares our...

First-Ever Malicious MCP Server Found in the Wild Steals Emails via

The first-ever malicious Model-Context-Prompt (MCP) server discovered in the wild, a trojanized npm package named postmark-mcp that has been secretly exfiltrating sensitive data from

Hackers turned OpenWebUI AI servers into crypto mining

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved

The researchers found a malware operation that''s been hijacking AI servers to mine cryptocurrency and steal sensitive credentials. The detected infections started by the end of 2024

Hackers Actively Exploit AI Deployments as 91,000+ Attack Sessions

The analysis reveals two distinct threat campaigns that systematically exploit the expanding surface area of AI deployments, ranging from server-side request forgery vulnerabilities to

''SymJack'' Attack Turns AI Coding Agents Into Supply Chain Attack ...

Artificial Intelligence ''SymJack'' Attack Turns AI Coding Agents Into Supply Chain Attack Delivery Systems Malicious repositories and disguised symlinks can trick AI coding agents into

Malicious MCP servers used in supply chain attacks | Securelist

In this article, we explore how the Model Context Protocol (MCP) — the new “plug-in bus” for AI assistants — can be weaponized as a supply chain foothold.

The First Malicious MCP Server in the Wild: A Wake-Up Call for AI ...

The malicious postmark-mcp server is more than an isolated incident—it''s a wake-up call. In a world where AI agents handle sensitive business functions, trust alone is no longer enough.

Hundreds of NPM packages compromised in a new

A major supply chain attack has compromised hundreds of open-source packages on NPM and PyPI, stealing developer credentials and wiping

First-ever AI-powered ''MalTerminal'' Malware uses

AI-powered malware, known as ''MalTerminal'', uses OpenAI''s GPT-4 model to dynamically generate malicious code, including ransomware and

AI-Generated Browser Ransomware Abuses Chromium API on

Cybersecurity researchers have flagged a new malware artifact generated using DeepSeek that constructed a novel attack path combining "unrealistic browser-malware concepts with a real

Malicious npm Packages Harvest Crypto Keys, CI Secrets, and API

As with prior Shai-Hulud attack waves, the malicious code embedded into the packages comes with capabilities to siphon system information, access tokens, environment secrets, and API

What we learned mapping a year''s worth of AI-enabled cyber threats

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved

As AI transforms the nature of and methods behind cyberattacks, how well do the techniques and frameworks used by the security community hold up? In a new report, we seek to

Researchers Find ChatGPT Vulnerabilities That Let Attackers Trick AI ...

Researchers Find ChatGPT Vulnerabilities That Let Attackers Trick AI Into Leaking Data | Read more hacking news on The Hacker News cybersecurity news website and learn how to protect

How to Recognize AI Attacks and Strategies for Securing Your AI ...

Cybercriminals are weaponizing AI using attacks like prompt injections, data poisoning, and jailbreak attempts. Security for AI is more critical than ever.

MCP Server Security: The Hidden AI Attack Surface | Praetorian

MCP server security is a critical blind spot in AI integration. Our researchers demonstrated code execution, data theft, and response manipulation — all invisible to users.

Adversarial Misuse of Generative AI

Much of the current discourse around cyber threat actors'' misuse of AI is confined to theoretical research. While these studies demonstrate the potential for malicious exploitation of AI,

Related Video Reference

This video was associated with the source search result. Verify technical details against current product documentation and project requirements.

Contact Us

Continue your research online:

Website: https://cgweb.co.za
Technical inquiry: https://cgweb.co.za/project-enquiry.html

This document is for preliminary research. Verify specifications against current standards, product documentation and project requirements.

© 2026 CGWEB NETWORK INFRASTRUCTURE - All rights reserved