# AI Server Security Issues

## Overview

This comprehensive guide explores the unique security challenges posed by AI agents and MCP servers, providing practical strategies and frameworks for building secure, resilient AI systems that enterprises can trust. The New Threat Landscape: Why AI Agent. Security researchers with AI security startup Cyata this week reported finding three vulnerabilities in the Git MCP server maintained by Anthropic, the AI company that created the Model Context Protocol to give AI models and agents a standardized way of accessing external data, tools, and services. Shadow AI refers to the unregulated use of AI technology within organizations, often without official oversight or security measures. As organizations adopt AI capabilities at an unprecedented rate, security teams must proactively gain visibility into AI usage and implement appropriate controls to mitigate risks. This includes everything from learning to problem-solving and, of course, decision-making. The system feeds massive amounts of data to AI systems.

## Article Content

Top 14 AI Security Risks in 2026

Discover the top 14 AI security risks in 2026 and learn how to mitigate them effectively with the support of SentinelOne.

The state of AI security in 2026

The evolution of AI infrastructure, including MCP servers and command-line interfaces (CLIs), have introduced a complicated attack surface at many organizations.

Anthropic, Microsoft MCP Server Flaws Shine a Light on AI Security ...

Post 1AI agents and MCP servers promise powerful automation, but they also introduce new and unfamiliar attack surfaces.According to recent findings highlighted by Security Boulevard,

MCP Security Issues Threatening AI Infrastructure | Docker

Learn about critical MCP security issues, their real-world horror stories, and how to best mitigate these rising vulnerabilities.

Azure AI security best practices | Microsoft Learn

This article provides best practices for securing AI workloads in Azure, including Azure OpenAI Service, Azure AI Foundry, and Azure Machine

AI coding agents keep repeating decade-old security mistakes

AI coding agents introduced vulnerabilities in 87% of pull requests across Claude, Codex, and Gemini builds, exposing access control gaps.

Security Archives | TechRepublic

Security Highlights Artificial Intelligence Vibe Coding Cheat Sheet: Tools, Prompts, Security Tips, and More

MCP ''design flaw'' puts 200k servers at risk: Researcher

A design flaw – or expected behavior based on a bad design choice, depending on who is telling the story – baked into Anthropic''s official Model Context Protocol (MCP) puts as many as

The Dark Side of AI: Data Security Threats & How to

This article breaks down the lesser-known AI data security risks—and how IT and security teams can stay ahead using smarter SaaS governance and

KB5082417

Overview KB5082417 is a cumulative security and reliability update for the Framework 3.5 and 4.8.1 released on April 14, 2026, targeting Windows 11 version 25H2 and

AI SECURITY CONCERNS IN A NUTSHELL

To thwart attacks, it is also essential to protect the input and output of the AI system from tampering, using measures on the hardware, operating system, and software level (in particular, installing

Enable AI assistance with Azure DevOps MCP Server

Learn about the Azure DevOps Model Context Protocol (MCP) Server, which enhances your AI assistant with real-time Azure DevOps context for smarter, more accurate project insights

Securing AI Agents and MCP Servers: A

This comprehensive guide explores the unique security challenges posed by AI agents and MCP servers, providing practical strategies and

Three high-risk AI vulnerabilities discovered in Claude.ai

Security experts flag multiple issues in Claude Code, warning, ''As AI integration deepens, security controls must evolve to match the new trust

April 14, 2026—KB5082142 (OS Build 20348.5020)

For more information about security vulnerabilities, see the Security Update Guide and the April 2026 Security Updates. Windows Server 2022 servicing stack update (KB5082137)

OneUptime | The Open-Source Observability Platform

OneUptime is an open-source complete observability platform. Monitor websites, APIs, and servers. Get alerts, manage incidents, and keep customers informed

MCP Servers Expose AI Agents to RCE Risk | Let''s Data Science

According to a whitepaper by Noma Security, reported by Help Net Security on May 5, 2026, many enterprise MCP servers and Skills introduce execution and data-risk vectors for AI

May 12, 2026—KB5089549 (OS Builds 26200.8457 and 26100.8457)

Improvements This update includes new features and quality improvements that were part of the following update: April 14, 2026—KB5083769 (OS Builds 26200.8246 and 26100.8246) April

Welcome to Channel Dive | Channel Dive

The team will be managed by me, in addition to my daily editorial duties at Light Reading. Our goal is to earn your trust as a fair and valuable

Why Server Security Risks Threaten AI Data Safety

Protect AI data with server security. Learn about threats, access controls, and defense strategies against attacks, breaches, and model risks.

Atlassian MCP Server

Atlassian MCP Server The Atlassian Rovo MCP Server is a cloud-based bridge between your Atlassian Cloud site and compatible external tools. Once configured, it enables those tools to

Claude Vulnerabilities Let Attackers Exfiltrate Sensitive

Three chained vulnerabilities in Claude.ai, Anthropic''s widely used AI assistant, that together allow attackers to silently exfiltrate sensitive conversation

Defender''s Guide to the Frontier AI Impact on Cybersecurity

Frontier AI models accelerate attacks. Learn the three-phase framework: Assessment, Protection, Platformization. Modernize security operations and match machine speed.

May 2026 Patch Tuesday forecast: AI starts driving security industry ...

Todd Schell from Ivanti gives his overview of April 2026 and forecast for May 2026 Patch Tuesday. Are you ready to get patching?

Vulnerabilities & Threats recent news | Dark Reading

Explore the latest news and expert commentary on Vulnerabilities & Threats, brought to you by the editors of Dark Reading

## Contact Us

For more information, pricing, or custom solutions, please contact us:

Website: https://www.fivesunsecoenergy.fr
Email: sales@fivesunsecoenergy.fr
Phone: +33 6 41 83 57 29
Address: 5 Rue de la Bourse, 75002 Paris, France

This document is for informational purposes only. Specifications subject to change without notice.