Severe Figma MCP Vulnerability Lets Hackers Execute Code Remotely — Patch Now

Cybersecurity researchers have disclosed details of a now-patched vulnerability in the popular figma-developer-mcp Model Context Protocol (MCP) server that could allow attackers to achieve code execution. The vulnerability, tracked as CVE-2025-53967 (CVSS score: 7.5), is a command injection bug stemming from the unsanitized use of user input, opening the door to a scenario where an attacker can send arbitrary system commands. "The server constructs and executes shell commands using unvalidated user input directly within command-line strings. This introduces the possibility of shell metacharacter injection (|, >, &&, etc.)," according to a GitHub advisory for the flaw. "Successful exploitation can lead to remote code execution under the server process's privileges." Given that the Framelink Figma MCP server exposes various tools to perform operations in Figma using artificial intelligence (AI)-powered coding agents like Cursor, an attacker could trick the MCP client to execute unintended actions by means of an indirect prompt injection. Cybersecurity company Imperva, which discovered and reported the problem in July 2025, described CVE-2025-53967 as a "design oversight" in the fallback mechanism that could allow bad actors to achieve full remote code execution, putting developers at risk of data exposure. The command injection flaw "occurs during the construction of a command-line instruction used to send traffic to the Figma API endpoint," security researcher Yohann Sillam said. The exploitation sequence takes place over through steps - The MCP client sends an Initialize request to the MCP endpoint to receive an mcp-session-id that's used in subsequent communication with the MCP server The client sends a JSONRPC request to the MCP server with the method tools/call to call tools like get_figma_data or download_figma_images The issue, at its core, resides in "src/utils/fetch-with-retry.ts," which first attempts to get content using the standard fetch API and, if that fails, proceeds to executing curl command via child_process .exec -- which introduces the command injection flaw. "Because the curl command is constructed by directly interpolating URL and header values into a shell command string, a malicious actor could craft a specially designed URL or header value that injects arbitrary shell commands," Imperva said. "This could lead to remote code execution (RCE) on the host machine." In a proof-of-concept attack, a remote bad actor on the same network (e.g., a public Wi-Fi or a compromised corporate device) can trigger the flaw by sending the series of requests to the vulnerable MCP. Alternatively, the attacker could trick a victim into visiting a specially crafted site as part of a DNS rebinding attack . The vulnerability has been addressed in version 0.6.3 of figma-developer-mcp, which was released on September 29, 2025. As mitigations, it's advisable to avoid using child_process .exec with untrusted input and switch to child_process .execFile that eliminates the risk of shell interpretation. "As AI-driven development tools continue to evolve and gain adoption, it's essential that security considerations keep pace with innovation," the Thales-owned company said. "This vulnerability is a stark reminder that even tools meant to run locally can become powerful entry points for attackers." The development comes as FireTail revealed that Google has opted not to fix a new ASCII smuggling attack in its Gemini AI chatbot that could be weaponized to craft inputs that can slip through security filters and induce undesirable responses . Other large language models (LLMs) susceptible to this attack are DeepSeek and xAI's Grok. "And this flaw is particularly dangerous when LLMs, like Gemini, are deeply integrated into enterprise platforms like Google Workspace," the company said . "This technique enables automated identity spoofing and systematic data poisoning, turning a UI flaw into a potential security nightmare." Found this article interesting? Follow us on Google News , Twitter and LinkedIn to read more exclusive content we post. artificial intelligence Command Injection cybersecurity Figma Imperva remote

code execution software security Vulnerability