Unofficial Postmark MCP npm silently stole users' emails - Against Invade

Data: 2025-09-25 21:08:38

Autor: Inteligência Against Invaders

A npm package copyingthe official ‘postmark-mcp’ project on GitHub turned bad with the latest

update that added a single line of code to exfiltrateall its users’ email communication.

Published by a legitimate-looking developer, the malicious package was a perfect replica of the authentic one in terms of code and description, appearing as an official port on npm for 15 iterations.

Model Context Protocol (MCP) is an open standard that allows AI assistants to interface with external tools, APIs, and databases in a structured, predefined, and secure manner.

Postmark is an email delivery platform, and Postmark MCP is the MCP server that exposes Postmark’s functionality to AI assistants, letting them send emails on behalf of the user or app.

As discovered by Koi Security researchers, the malicious package on npm was clean in all versions through1.0.15, but in the 1.0.16 release, it added a line that forwarded all user emails to an external address at giftshop[.]club linked to the same developer.

[IMAGEM REMOVIDA]
[IMAGEM REMOVIDA]vulnerability or misconfigurationcarries a significant risk.

Users should verify the source of the project and make sure it’s an official repository, review the source code and changelogs, and look carefully for changes in every update.

Before using a new version in production, run MCP servers in isolated containers or sandboxes and monitor their behavior for suspicious actions like data exfiltration or unauthorized communication.