

Abstract —

AI-assisted “vibe coding” tools have made it easier and faster than ever to build software, but they also introduce new security risks into the open-source supply chain. Code generated by AI can unknowingly include unverified, outdated, or even hallucinated dependencies, which increases the chances of malicious packages, typosquatting attacks, and vulnerable libraries being pushed to public repositories.

To address this, **VibeScan** is introduced as a cross-platform, pre-publish security analysis tool available as both a Python package and a Node.js package. It is designed to fit naturally into modern development workflows and helps developers catch risky dependencies before their code is published. VibeScan analyzes project dependencies using a combination of heuristic rules, static code analysis, and machine-learning-based risk scoring to detect suspicious packages, unsafe installation behavior, and unusual dependency patterns.

The tool can be used as a command-line utility, a pre-commit hook, or a CI/CD check, allowing teams to enforce security checks early and consistently. By generating clear, explainable risk scores and structured security reports across both ecosystems, VibeScan shifts security checks earlier in the development lifecycle and helps reduce supply-chain risks introduced by AI-generated code.

Overall, VibeScan provides a practical, developer-friendly way to add trust and safety to the AI-driven coding process without slowing developers down.