CodeGate protects the privacy of developers that use AI coding assistants

New open source project from the creators of Kubernetes and Sigstore prevents secrets leakage and protects code from risky dependencies

SEATTLE, WA, UNITED STATES, December 23, 2024 /EINPresswire.com/ -- More than 90% of developers now use AI coding assistants—the primary motivator is the potential to produce more code and ship faster. However, AI coding assistants like GitHub Copilot and Cursor have under-recognized shortcomings.

> It was important that CodeGate be open source. Of course, our company's DNA is open source, but in particular our belief is that when you're addressing privacy and security, a solution must be open."
>
> *Luke Hinds, cofounder and CTO at Stacklok*

"AI coding assistants are chatty. I have seen many instances where they grab data, passwords and other secrets and pass them on to large language models," said Luke Hinds, cofounder and CTO at Stacklok. "The risk of course is that your secrets are now part of the training dataset for public models. We built CodeGate to prevent any accidental exposure of secrets, recognizing this was an important start point in creating value for developers."

CodeGate is a new open source project from the team at Stacklok. CodeGate offers software developers that use AI coding assistants their own local privacy controls. Specifically, CodeGate is a single, lightweight container that sits between the AI coding assistant and the large language model; it identifies and encrypts any secrets before they reach the model, and it decrypts those secrets upon return.

"Developers that use AI coding assistants face another critical issue," warned Hinds. "Large language models have training cutoff dates that are typically 12 or more months in the past. That means they lack up-to-date knowledge of dependencies that have become deprecated or dangerous; they can recommend or even merge these high-risk dependencies into code."

CodeGate maintains a constantly updated database of known malicious packages and deprecated dependencies; it augments prompts with up-to-date security information using RAG (research augmented generation) and blocks any recommendations that dangerous packages be used. CodeGate also provides developers with proven, safe alternatives.

Hinds and Stacklok co-founder Craig McLuckie both have long histories with open source software. Hinds founded the Sigstore project, which was later joined by Google and others, and McLuckie was a co-founder of Kubernetes and the CNCF (Cloud Native Computing Foundation).

“It was important to us that CodeGate be open source. Of course, our company’s DNA is open source, but in particular our belief is that when you’re addressing privacy and security, a solution must be open,” noted Hinds. “Open source software is freely available to inspect and modify, and ultimately, this allows us to advance the solution—and developer interests—with the community.”

For more information about CodeGate, visit codegate.ai, or to engage directly with the project, explore the GitHub repository.

About Stacklok

Stacklok brings developers and security teams together to eliminate all forms of risk before code is merged. Stacklok provides security professionals with control of policy across the entire software development lifecycle to continuously and consistently secure software projects. And Stacklok empowers developers with intelligence on high-risk open source packages as part of their existing workflows, so they can make safer open source choices. Stacklok is led by creators of Kubernetes and Sigstore, solving for open source software security through deep connection and collaboration with the community.

Scott Buchanan
Stacklok
email us here
Visit us on social media:
X
LinkedIn
YouTube
