

Secsys-FDU / LLM-Tool-Calling-CVEs Public[Code](#) [Issues 12](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#) [Insights](#)[New issue](#)

HAI Build Code Generator Remote Code Execution Vulnerability #10

[Open](#)

Secsys-FDU opened 3 days ago

[Owner](#)

Vulnerability type : Other or Unknown

Other vulnerability type : CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vendor of the product(s) : HAI Build Code Generator

Affected Product: HAI Build Code Generator (<https://github.com/presidio-oss/hai-build>)

Affected Version : <= 3.13.3

Attack Type : Remote

Impact : Code Execution

Affected component : Tool Call Parser, Command Validation Logic, Auto-Execution Module

Description

In its design for automatic terminal command execution, HAI Build Code Generator offers two options: Execute safe commands and Execute all commands. The description for the former states that commands determined by the model to be safe will be automatically executed, whereas if the model judges a command to be potentially destructive, it still requires user approval. However, this design is highly susceptible to prompt injection attacks. An attacker can employ a generic template to wrap any malicious command and mislead the model into misclassifying it as a 'safe' command, thereby bypassing the user approval requirement and resulting in arbitrary command execution.

[Sign up for free](#) to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

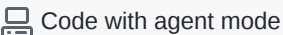

Milestone

No milestone

Relationships

None yet

Development

 Code with agent mode 

No branches or pull requests

Participants

