New issue

DSAI-Cline Remote Code Execution Vulnerability #9

Open

Secsys-FDU opened last week 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)：DSAI-Cline
Affected Product: DSAI-Cline (https://github.com/necboy/cline-DSAI)
Affected Version：<= 1.1.2

Attack Type：Remote
Impact：Code Execution
Affected component：Tool Call Parser, Command Validation Logic, Auto-Execution Module

Description
DSAI-Cline's command auto-approval module contains a critical OS command injection vulnerability that renders its whitelist security mechanism completely ineffective. The system relies on string-based parsing to validate commands; while it intercepts dangerous operators such as ;, &&, ||, |, and command substitution patterns, it fails to account for raw newline characters embedded within the input.
An attacker can construct a payload by embedding a literal newline between a whitelisted command and malicious code (e.g., git log\nmalicious_command), forcing DSAI-Cline to misidentify it as a safe operation and automatically approve it. The underlying PowerShell interpreter treats the newline as a command separator, executing both commands sequentially, resulting in Remote Code Execution without any user interaction.

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