

AI coding agents' 0-click RCE flaw could hand attackers keys to the kingdom

SECONDARY

Publisher The Register

Published 2026-09-17

Retrieved 2026-09-21

Cite key theregister2026ai

URL https://www.theregister.com/security/2026/09/17/ai_coding_agents_0-click_rce_flaw_could_h_and_attackers_keys_to_the_kingdom/

Assessment. Same-day trade coverage. Adds that GitHub implemented SHA-name restrictions at the forge and that Google points Gemini CLI users at Antigravity CLI. Used only to corroborate details the primary source also carries.

The Register, 17 September 2026.

Disclosed by Air, a security startup specialising in enterprise AI agent protection. Reported to vendors June 2026.

"The agent checks out the exact commit the marketplace pinned but never verifies it landed there."

Affected: Anthropic Claude Code, OpenAI Codex, Google Gemini CLI, GitHub Copilot.

Anthropic: Claude Code 2.1.179 patched. OpenAI: Codex 0.146.0 patched. Google: deprecated Gemini CLI, directing users to Antigravity CLI. Microsoft: no patch for Copilot; GitHub implemented SHA-name restrictions.

Two exploitation routes: submit a benign plugin that later receives a malicious update, or hijack a legitimate repository and push a compromised version to all installed instances.