

AI coding agents leaked 13,000 internal company screenshots to public GitHub repos

SECONDARY

Publisher Help Net Security

Published 2026-09-30

Retrieved 2026-10-02

Cite key helpnetsecu2026ai

URL <https://www.helpnetsecurity.com/2026/09/30/ai-coding-agents-github-screenshot-leak/>

Claims drawn from this source. CLAIM-2026-10-02-01, CLAIM-2026-10-02-02, CLAIM-2026-10-02-03, CLAIM-2026-10-02-08

Research by Glow Labs, reported as "PixelLeak". 13,000+ internal images, 900+ code repositories, 300+ organisations, 100+ public accounts with exposed internal work. Researchers began notifying affected organisations on 9 September 2026.

Affected organisations described but not named: "one of the world's largest tech companies, a frontier AI lab, a major enterprise software provider and a Fortune 500 travel company".

Mechanism: developers asked AI agents to verify UI fixes with screenshots. Because GitHub's pull request image upload worked only in browsers and not from the command line, some agents created public repositories under developers' personal accounts to host the images.

gitshot named as the tool used by about one-third of affected organisations. Claude Code with the Opus 5 model reproduced the behaviour in lab testing. Data exposed included billing records and screenshots of unreleased features, treasury consoles, institutional client withdrawal screens and utility company billing records. Remediation: "Hardening AI tool configurations is key for prevention."