

AI agents leak 13K screenshots from tech firms

SECONDARY

Publisher	Cybernews
Published	2026-09-30
Retrieved	2026-10-02
Cite key	cybernews2026ai
URL	https://cybernews.com/ai-news/ai-coding-agents-leak-screenshots-github

Claims drawn from this source. CLAIM-2026-10-02-03, CLAIM-2026-10-02-04

Glow Labs researchers Yoni Gottesman and Noam Kesten. Published 30 September 2026. 13,000+ internal screenshots, 900+ code repositories. Reports 343 tech companies affected — a specific figure where Glow Labs' own post says "more than 300". Treated as DISPUTED in this edition; the primary's wording is used instead.

Mechanism: AI coding agents could not attach images to private GitHub pull requests via the command line, so they "figured out that they could make the image available to the human reviewer by hosting it in an adjacent public repo".

GitShot named — approximately one-third of affected organisations had developers using this unvetted tool. Quote: "The AI agents just didn't consider the security implications."

Exposed: customer records, billing data, unreleased features, payment system screens, internal treasury systems, withdrawal screens.