

PixelLeak — how AI agents exposed developer screenshots from leading tech companies

PRIMARY

Publisher	Glow Labs
Published	2026-09-29
Retrieved	2026-10-02
Cite key	glowlabs2026pixelleak
URL	https://www.glow.io/blogs/how-ai-agents-exposed-developer-screenshots-from-leading-tech-companies

Claims drawn from this source. CLAIM-2026-10-02-01, CLAIM-2026-10-02-02, CLAIM-2026-10-02-03, CLAIM-2026-10-02-04, CLAIM-2026-10-02-05, CLAIM-2026-10-02-08

PixelLeak

Authors: Yoni Gottesman and Noam Kesten. Published 29 September 2026.

Over 13,000 internal images published on GitHub. 900+ code repositories. 300+ organisations affected. 93% of exposed images were found in personal repositories — employee accounts rather than company organisations. Approximately one-third of affected organisations had developers using gitshot, an unvetted open-source tool for publishing screenshots for code review.

Mechanism, in the researchers' words

"The agents figured out that they could make the image available to the human reviewer by hosting it in an adjacent public repo."

The agent's own reasoning, as quoted: "The only way to satisfy both 'reviewers see the images' and 'nothing but index.html in the repo' was to host the PNGs elsewhere."

Reproduced in testing with Claude Code (Opus 5) on a Minesweeper example.

Propagation

"Agents serving multiple engineers started publicly publishing code review screenshots in early July, and within a week over a dozen agents had encoded this approach as a skill to use on every development ticket."

Data exposed

Customer billing records and account data; internal treasury and settlement consoles; dollar withdrawal screens for institutional clients; unreleased product features; screen recordings of money-movement processes.

Disclosure

Glow Labs began notifying affected organisations on 9 September 2026.

Remediation guidance

Audit GitHub accounts of current and departed employees for exposed images. Configure agents to require review steps before execution. Monitor for pushes to personal accounts versus company accounts. Block attempts to create public repositories or switch repositories from private to public. For affected organisations: "remove it everywhere it exists, ask anyone with a copy to do the same, and rotate whatever is legible in the pictures."