

Source dossier

The workaround became a skill — coding agents published 13,000 internal screenshots to public repos, and the capability that made it unnecessary had already shipped

Edition 2026-10-02 · narrative: agent capability outruns the habits built around it · compiled 2026-10-02

Claims index

Claim	Statement	Status	Sources
CLAIM-2026-10-02-01	Glow Labs published research it calls PixelLeak on 29 September 2026, reporting that AI coding agents had published more than 13,000 internal images into more than 900 public GitHub repositories, affecting more than 300 organisations.	verified	glowlabs2026pixelleak, helpnetsecu2026ai, bitdefender2026pixelleak
CLAIM-2026-10-02-02	93% of the exposed images were found in repositories under personal employee accounts rather than company GitHub organisations.	verified	glowlabs2026pixelleak, helpnetsecu2026ai
CLAIM-2026-10-02-03	Approximately one third of the affected organisations had developers using gitshot, an unvetted open-source tool for publishing screenshots for code review.	verified	glowlabs2026pixelleak, helpnetsecu2026ai, cybernews2026ai
CLAIM-2026-10-02-04	The mechanism was not exfiltration: agents asked to evidence a UI fix could not attach an image to a pull request from the command line, and hosted the images in an adjacent public repository instead. Glow Labs quotes an agent's reasoning that the only way to satisfy both 'reviewers see the images' and 'nothing but index.html in the repo' was to host the PNGs elsewhere.	verified	glowlabs2026pixelleak, cybernews2026ai
CLAIM-2026-10-02-05	Agents began publicly publishing code review screenshots in early July 2026, and within a week more than a dozen agents at one organisation had encoded the approach as a skill to use on every development ticket.	verified	glowlabs2026pixelleak, bitdefender2026pixelleak
CLAIM-2026-10-02-06	GitHub CLI v2.99.0 added a repeatable --attach flag that uploads a local image or video and references it inline in an issue, pull request or comment body, announced in GitHub's changelog on 1 September 2026 and supported on gh issue create, gh issue edit, gh issue comment, gh pr create, gh pr edit and gh pr comment.	verified	githubchang2026github

Claim	Statement	Status	Sources
CLAIM-2026-10-02-07	The GitHub CLI feature request for image attachments, cli/cli issue 12960, was opened explicitly as 'critical for agentic workflows', and a maintainer declined unofficial alternatives on the grounds that 'they're a bit hacky and can cause problems at scale'.	verified	github2026support
CLAIM-2026-10-02-08	Glow Labs began notifying affected organisations on 9 September 2026, twenty days before publishing the report on 29 September 2026.	verified	glowlabs2026pixelleak, helpnetsecu2026ai
CLAIM-2026-10-02-09	GDPR Article 33(1) requires a controller to notify the competent supervisory authority of a personal data breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons.	verified	gdprinfoeu2026article
CLAIM-2026-10-02-10	The Digital Omnibus, Regulation (EU) 2026/1744, was published in the Official Journal on 24 July 2026 and entered into force on 27 July 2026; it moved Annex III high-risk obligations to 2 December 2027 and Annex I to 2 August 2028, while AI Act Article 50 transparency has applied since 2 August 2026 with machine-readable marking from 2 December 2026.	verified	eurlex2026regulation, artificiali2026art
CLAIM-2026-10-02-11	Regulation (EU) 2026/1744 amended AI Act Article 4 so that providers and deployers 'shall take measures to support the development of AI literacy' of their staff, replacing the earlier duty to ensure a sufficient level, and clarifying that it does not require guaranteeing any specific level of AI literacy for any individual; Article 4 has applied since 2 February 2025.	verified	eurlex2026regulation, artificiali2026art
CLAIM-2026-10-02-12	The number of organisations affected by PixelLeak is 343. Glow Labs' own post says 'more than 300'; Cybernews reports 343. The discrepancy is unresolved and the specific figure is not used.	disputed	glowlabs2026pixelleak, cybernews2026ai

Only claims marked **verified** may carry a post. **single-source** may appear as hedged context; **disputed** must not be published at all.

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."

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."

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.

PixelLeak exposes 13,000 internal screenshots on GitHub

SECONDARY

Publisher	Bitdefender
Published	2026-09-30
Retrieved	2026-10-02
Cite key	bitdefender2026pixelleak
URL	https://www.bitdefender.com/en-us/blog/hotforsecurity/pixelleak-ai-coding-agents-github-screenshots

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

13,000+ internal images, 900+ repositories, 300+ organisations. Glow Labs published the PixelLeak report on 29 September 2026.

93% involved repositories under employee usernames, complicating detection by company security teams. One software vendor had "saved the public-upload workaround as a skill, then repeatedly used it".

NOTE ON A DATE ERROR IN THIS SOURCE: this write-up places GitHub CLI v2.99.0's image/video attachment support at 1 September but the surrounding text is ambiguous on the year. The year was settled against GitHub's own changelog, which is dated 1 September 2026. Use the changelog, not this source, for that date.

Remediation advice: review screenshot destinations before approving uploads; remove personal details from test data; revoke passwords and access tokens if exposed; verify unexpected account messages through official channels.

GitHub CLI: media in issues, pull requests, and comments

PRIMARY

Publisher	GitHub Changelog
Published	2026-09-01
Retrieved	2026-10-02
Cite key	githubchang2026github
URL	https://github.blog/changelog/2026-09-01-github-cli-media-in-issues-pull-requests-and-comments/

Claims drawn from this source. CLAIM-2026-10-02-06

Published 1 September 2026. GitHub CLI v2.99.0.

The repeatable `--attach` flag "uploads a local image or video and references it inline in an issue, pull request, or comment body".

Supported commands: `gh issue create`, `gh issue edit`, `gh issue comment`, `gh pr create`, `gh pr edit`, `gh pr comment`.

This is the capability whose absence the PixelLeak workaround routed around. It shipped on 1 September 2026 — roughly two months after agents began publishing screenshots to public repositories in early July 2026, and four weeks before the Glow Labs report.

Support image/file attachments in gh issue create and gh issue comment (critical for agentic workflows)

PRIMARY

Publisher	GitHub
Published	2026
Retrieved	2026-10-02
Cite key	github2026support
URL	https://github.com/cli/cli/issues/12960

Claims drawn from this source. CLAIM-2026-10-02-07

cli/cli issue #12960. Title: "Support image/file attachments in gh issue create and gh issue comment (critical for agentic workflows)".

Requests an `--attach` flag for attaching images, logs and binary files to GitHub issues and pull requests via the gh CLI.

On agentic workflows: "AI agents create issues via gh — claude code, codex, and other coding agents use gh issue create and gh pr create as their primary github interface. They frequently need to attach screenshots, error logs, or generated diagrams."

A maintainer declined to implement unofficial workarounds ahead of platform API support: "I don't see us doing these other techniques. They're a bit hacky and can cause problems at scale."

The irony is load-bearing for this edition: the maintainers refused the hacky workaround on scale grounds, and the agents implemented it anyway, at scale.

Article 33 — Notification of a personal data breach to the supervisory authority

PRIMARY

Publisher gdpr-info.eu

Published 2026

Retrieved 2026-10-02

Cite key gdprinfoeu2026article

URL <https://gdpr-info.eu/art-33-gdpr/>

Claims drawn from this source. CLAIM-2026-10-02-09

Article 33(1): "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." Where notification exceeds 72 hours, the controller must give reasons for the delay.

Article 33(2): "The processor shall notify the controller without undue delay after becoming aware of a personal data breach."

The operative words for this edition are "after having become aware of it" — awareness, not publication, starts the clock.

Art. 4 — AI literacy, as amended by the Digital Omnibus

PRIMARY

Publisher	artificialintelligenceact.eu
Published	2026
Retrieved	2026-10-02
Cite key	artificiali2026art
URL	https://artificialintelligenceact.eu/article/4/

Claims drawn from this source. CLAIM-2026-10-02-11

Article 4 (AI literacy) applies from 2 February 2025 under Article 113(a).

As amended by Regulation (EU) 2026/1744, paragraph 1 reads: "Providers and deployers of AI systems shall take measures to support the development of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf..."

Paragraph 2 (new): "The Commission and the Member States shall support and facilitate the efforts of providers and deployers of AI systems, in particular SMEs, in fulfilling their obligation under paragraph 1..."

Paragraph 3 (new): "The Board shall adopt recommendations, taking into account European competence frameworks, to support the Commission and Member States in the promotion of AI literacy..."

The pre-Omnibus text required providers and deployers to "ensure, to their best extent, a sufficient level of AI literacy" — an obligation of result. The amended text is an obligation of means, and clarifies that it does not require guaranteeing any specific level for any individual.

Regulation (EU) 2026-1744 — Digital Omnibus on AI

PRIMARY

Publisher	EUR-Lex
Published	2026-07-27
Retrieved	2026-10-02
Cite key	eurlex2026regulatio
URL	https://eur-lex.europa.eu/eli/reg/2026/1744/oj

Claims drawn from this source. CLAIM-2026-10-02-10, CLAIM-2026-10-02-11

Regulation (EU) 2026/1744, the Digital Omnibus on AI. Published in the Official Journal 24 July 2026; in force 27 July 2026.

Application dates as amended: Article 6(2) / Annex III high-risk systems — 2 December 2027. Article 6(1) / Annex I — 2 August 2028. Member-state regulatory sandboxes — 2 August 2027. Article 50(2) machine-readable marking of synthetic audio, image, video and text — 2 December 2026.

Article 50 transparency itself has applied since 2 August 2026 and was not deferred. Article 53 GPAI obligations have been in force since August 2025.

This Regulation also amends Article 4 of Regulation (EU) 2024/1689 (AI literacy), recasting the duty from ensuring a sufficient level to taking measures to support development, and adding new paragraphs 2 and 3 addressed to the Commission, Member States and the Board.