

The AG Gazette

Models, machines, and matters of consequence

PARIS, SATURDAY 17 OCTOBER 2026

MORNING EDITION · No. 2026-10-17-MORNING

ISSUED 06:26 CEST

PRICE: COMPLIMENTARY

MORNING EDITION — SATURDAY 17 OCTOBER 2026

Reporting window: 16 Oct 2026, 16:09 CEST to 17 Oct 2026, 06:26 CEST (Paris time). Issued 17 Oct 2026, 06:26 CEST.

Four material developments have primary publication timestamps after the actual October 16 afternoon edition at 16:09 CEST: Claude's reconstruction of NIST curve-seed origins, Anthropic's quantum-circuit results and internal employment study, and Claude Code 2.1.302. A separate BACKGROUND dispatch covers Google's October 16 wet-lab research; its publication hour is unavailable, so it is not claimed as post-cutoff news. Beam is not repeated. No additional model or policy launch cleared the timing and primary-source verification gates.

4 NEW OR UPDATED DISPATCHES · 1 BACKGROUND ITEM · PREVIOUS: [2026-10-16-AFTERNOON](#)

THE NEWS

CODING & AGENTS NEW

CLAUDE CODE 2.1.302 LIMITS IMAGE READS AND CHANGES DEFAULT PERMISSION BEHAVIOR

PUBLISHED: 16 Oct 2026, 22:53 CEST

Anthropic published stable Claude Code 2.1.302 on October 16 at 22:53 CEST. The release fixes the Read tool loading arbitrarily large images, or pipes and devices named like images, entirely into memory. Image sources larger than 128 MB are now refused.

The changelog says headless claude -p and Agent SDK sessions without an explicit permission mode now start in default mode on third-party providers, with telemetry off or on a fresh install; explicitly selecting auto mode keeps it. A separate setting, CLAUDE_CODE_AUTO_MODE_MODEL, chooses the client-side auto-mode classifier model and does not change the server-side classifier.

The release also fixes MCP servers returning no tools or failing calls when negotiating protocol version 2026-07-28 without resultType, ttlMs or cacheScope. It fixes cloud-session scheduled runs unexpectedly restarting an hour or more after a partial failure, a behavior the changelog says could repeat work such as posting a report twice.

ANALYSIS — WHY IT MATTERS. *Operators of unattended agents should review explicit permission settings and duplicate-action protections. Input-size limits and clearer failure states matter independently of model capability.*

CAVEAT. These are vendor-documented changes, not a security audit or an installation recommendation. We verified the official release metadata and notes; we did not install the version or reproduce every fix. Codex 0.164.0 builds found this morning are prereleases with sparse notes, not a verified stable feature launch.

SOURCES

1. Claude Code official release metadata

https://api.github.com/repos/anthropics/claude-code/releases?per_page=5 (primary source) **CHECKED:** 17 Oct 2026, 06:11 CEST

RESEARCH NEW

CLAUDE RECONSTRUCTS NIST CURVE-SEED ORIGINS, NOT AN ECDSA VULNERABILITY

PUBLISHED: 16 Oct 2026, 19:02 CEST

Anthropic published a reproducible explanation for the seeds behind the NIST P-192, P-224, P-256, P-384 and P-521 elliptic curves. Its internal research model identified output from the C-library lrand48 pseudorandom generator initialized with Unix timestamps, rather than the rumored hash of a humorous passphrase. The article's publication timestamp is October 16 at 19:02 CEST, after the previous edition.

The company says the initial discovery took under half an hour. Its article includes code for regenerating the seeds and explains some selected base points. For this edition, an independent local implementation of the published timestamp-and-generator recipe reproduced the exact standardized P-256 seed. That is a narrow computational check, not an independent reconstruction of the whole investigation.

Anthropic explicitly says this is not a cryptographic break, a new attack or a reason to change ECDSA deployments. It argues the simple generation method reduces concerns about deliberately selected weaknesses. Important questions remain: B-163's seed is unexplained, several base-point origins remain unknown, and the reason some apparently viable curve candidates were skipped is not established.

ANALYSIS — WHY IT MATTERS. *A transparent, reproducible origin story helps distinguish parameter-provenance concerns from actual cryptographic vulnerabilities. Security teams should read the result as new evidence about historical choices, not as an emergency migration advisory.*

CAVEAT. The investigation and broader security interpretation are Anthropic's. Our local verification reproduced only P-256's seed. The findings do not constitute a proof that every curve-selection decision was innocuous, nor do they recover private keys.

SOURCES

1. Anthropic research and reproduction code

<https://www.anthropic.com/research/ecdsa-curve-origins> (primary source) **CHECKED:** 17 Oct 2026, 06:22 CEST

ANTHROPIC REPORTS NEW QUANTUM-CIRCUIT DESIGNS, INCLUDING A 17-FOLD GATE REDUCTION

PUBLISHED: 16 Oct 2026, 19:29 CEST

Anthropic's October 16 research announcement, published at 19:29 CEST, describes evaluator-guided quantum-circuit design using Claude Mythos 5. The model received plain-language specifications, proposed implementations, and iterated against a program that checked correctness and scored resource use across eight computational primitives.

The associated preprint was submitted to arXiv on October 15 at 17:59 UTC. Its abstract reports reductions in both Toffoli gates and qubits on seven tasks; the eighth produced a new reversible architecture for prime-field modular inversion. This edition treats the October 16 announcement as the new event and preserves the paper's earlier submission date.

In one design trade-off, the announcement reports 17 times fewer gates while using 12% more qubits than the smallest previous design. For a Reed-Solomon decoder used in decoded quantum interferometry, it reports a 12-fold gate reduction relative to a previous Google construction. These are specific circuit-resource comparisons, not a claim that all quantum algorithms are 17 times faster.

The modular-inversion search ran for 53 hours with an initial brief and occasional human prompts to broaden its approach. The decoder reserves less storage by accepting rare failures, about one in 10,000 sampled cases under the stated allowance. An external evaluator here means a separate checking program, not independent replication by another research group.

ANALYSIS — WHY IT MATTERS. *Verifiable code and explicit resource objectives can make a well-defined scientific optimization task suitable for an iterative agent. Lower circuit costs could help future hardware, but do not themselves demonstrate useful quantum advantage on today's machines.*

CAVEAT. The paper is a preprint and the numerical results are the authors' reports. We verified the primary announcement, abstract and submission history, not every circuit or the full experimental artifact. Resource trade-offs, allowed failure rates and human interventions matter; this is not evidence of unrestricted autonomous scientific discovery.

SOURCES

- 1. Anthropic quantum-circuit announcement**
<<https://www.anthropic.com/research/designing-efficient-quantum-circuits>> (primary source) **CHECKED: 17 Oct 2026, 06:18 CEST**
- 2. Paper and original submission history**
<<https://arxiv.org/abs/2610.22367>> (primary source) **CHECKED: 17 Oct 2026, 06:18 CEST**

ANTHROPIC REPORTS SIX AGENT-HOURS PER HUMAN-HOUR, ALONGSIDE A FALLING JUNIOR-HIRING SHARE

PUBLISHED: 16 Oct 2026, 18:26 CEST

An internal employment study published by Anthropic on October 16 at 18:26 CEST says employee-directed interactive agents logged six times the company's estimated human work hours by August. The numerator is agent runtime, including inference and active tool use, pooling subagents and excluding waits longer than 30 minutes. Human hours are estimated from headcount at 40 hours per week. This is not a finding that agents were six times as productive as people.

The study reports that junior employees' share of technical headcount fell from 21% to 14% since early 2025, while juniors' share of technical hires fell from 27% to 9%. Technical hiring still grew in absolute terms as the company expanded. A decline in hiring share is not equivalent to an observed count of jobs eliminated.

To examine coding-tool adoption, the authors follow 192 adopting engineers and compare them with 74 non-adopters. They report rising code output, but acknowledge that adoption was not randomized and that more code does not necessarily mean more business impact. Their code-quality proxies include later deletions and reversions, not a comprehensive independent quality assessment.

The report describes human attention as a bottleneck. One interviewed engineer called the experience 'an army of Claudes, with every one asking for my attention.' It also reports that interactive sessions spent around 80% of wall-clock time waiting for human input. That idle-time measure is distinct from the active agent-hours ratio.

ANALYSIS — WHY IT MATTERS. *This is a concrete case study of how agent adoption can shift work toward orchestration, review and judgment. Its measurement definitions are as important as the headline ratios when evaluating staffing or productivity claims.*

CAVEAT. This is a single rapidly growing AI vendor studying itself, with internal data and 17 employee interviews. Selection, revenue growth, organizational change and non-random tool adoption limit causal inference and generalization. We did not access private employee or candidate records, and this reporting makes no changes to Job Alerts.

SOURCES

- 1. Anthropic employment study and methodology**
<<https://www.anthropic.com/research/employment-at-anthropic>> (primary source) **CHECKED: 17 Oct 2026, 06:22 CEST**

BACKGROUND — OLDER OR UNDATED CONTEXT

Earlier or undated items, carried for context only. They are not new reporting.

RESEARCH

BACKGROUND — OLDER CONTEXT

BACKGROUND: GOOGLE REPORTS SUPERVISED LAB-IN-THE-LOOP ADVANCES, NOT A FULLY AUTONOMOUS WET LAB

PUBLISHED: 16 Oct 2026

BACKGROUND - original publication October 16, 2026. Google Research describes three projects connecting AI agents to biological experiments: the VERID laboratory digital twin and robotics safeguards, closed-loop aptamer discovery, and de novo protein-binder design. The page gives no publication hour we could verify, so this dispatch is not claimed as a development after the previous edition.

For aptamers, the team reports three design-test cycles with final confirmed on-target hit rates of 33.5% for myoglobin and 42.1% for alpha-thrombin. The myoglobin experiment initially got worse when designs favored nonspecific sticky binders, then recovered after revising the design rules. These two targets and experimental cycles do not establish general reliability across biology.

The protein-binder work reports more than an eightfold computational-cycle acceleration and single-digit nanomolar affinity against FAP. Google's next step is to combine the projects: the post does not say the complete integrated autonomous lab already exists. Safeguards include sequence screening, simulated robot runs, human authorization of sequences and protocols, and supervision of execution.

ANALYSIS — WHY IT MATTERS.

Real experimental feedback can expose shortcuts that look successful in simulation. The reported failure-and-recovery sequence is more informative about the scientific workflow than an undifferentiated claim that AI has automated a laboratory.

CAVEAT. These are results reported by Google, not replicated by this newspaper. Tight binding is not proof of a clinically useful drug. Integration remains future work, and the experiments retain human oversight. This older, newly verified context is explicitly separated from the four timed new developments.

SOURCES

1. Google Research original wet-lab report

<https://research.google/blog/grounding-ai-agents-in-biological-reality-building-blocks-for-autonomous-wet-labs/>

(primary source)

CHECKED: 17 Oct 2026, 06:16 CEST

KEY PATTERNS — EDITORIAL ANALYSIS

- Reproducible artifacts and separate correctness checks support narrower conclusions than sweeping capability claims.

— Active agent runtime is not human-equivalent productivity; explicit definitions and selection limits matter.

— Permission defaults, bounded input reads and duplicate-run fixes are operationally important agent-release changes.

SOURCE COVERAGE & COLOPHON

COLLECTION ENGINE VERSION: 3.28.0 RAN THIS EDITION: yes ENGINE LOOK-BACK: 2 days	SOURCE STATUS REDDIT: ok YOUTUBE: ok HACKERNEWS: ok POLYMARKET: unreachable GITHUB: ok DEVTO: ok
COVERAGE NOTES — The new-development window begins at the actual October 16 afternoon issue, 16:09 CEST. Four primary publication timestamps are later than that cutoff. One October 16 date-only scientific report	ENGINE FOOTER --- All agents reported back! — Reddit: 22 threads 4,234 upvotes 1,357 comments — YouTube: 4 videos 457,324 views 4/4 with transcripts

is separately labeled BACKGROUND; no fresh event is inferred from a discussion or crawl date.

- The installed last30days engine completed successfully with 54 discovery items across five returning sources. Discovery covered models, coding and agents, research, industry, infrastructure and policy. Evidence items are not counts of verified news developments.
- Polymarket was unreachable because TLS hostname verification failed; verification was not bypassed. X was not configured and was omitted. The four retained YouTube videos have transcripts; a fifth candidate failed subtitle retrieval after HTTP 429 responses before relevance filtering.
- Three post-engine native web supplements were run, with empty-result queries retried more broadly. The configured search backend was unavailable; its automatic keyless fallback supplied the returned results. Direct HTTPS retrieval with normal certificate validation supplied primary articles, metadata and source snapshots because the text extractor was unavailable.
- No additional post-cutoff model launch was established. Beam was covered yesterday; Meta Muse Spark Open is dated October 15. The NVIDIA Indic corpus announcement is timestamped October 16 at 03:44 CEST and says the corpus is releasing soon. Sparse Codex alpha release notes were not treated as a stable feature launch.
- China export-control discussion was found, but primary legal text and publication timing were not verified in this run. It is not presented as enacted policy. Other older papers, resurfaced commentary and undated claims were not promoted to fresh developments.
- Available community comments concern other or older topics, not these selected new events. We do not attach them to unrelated announcements or claim a representative consensus. The quoted workplace interview is attributed to the primary study, not labeled community reaction.
- No browser-cookie access, optional services or credentials, paid enrichment, TLS bypass, job-alert edits or schedule changes were used. Full research, source snapshots and provenance remain private.

THIS EDITION

- [Exact input JSON](#)
- [Markdown text](#)
- [Permanent page](#)

- HN: 18 stories | 710 points | 481 comments
- dev.to: 4 articles | 33 reactions | 22 comments
- GitHub: 6 items | 17 reactions | 54 comments
- Top voices: r/artificial, r/singularity, r/LocalLLaMA

The AI Gazette is a locally rendered digest. Each dispatch separates reported facts, labeled analysis and caveats, and cites the sources checked at the times shown. Background items are older or undated context, not new reporting.

Rendered as static HTML with inline styles and no scripts, cookies or analytics. Typefaces are requested from Google Fonts (fonts.googleapis.com, fonts.gstatic.com); if that request is blocked, Georgia, Times or another installed serif is used.