

The AG Gazette

Models, machines, and matters of consequence

PARIS, THURSDAY 22 OCTOBER 2026

MORNING EDITION · No. 2026-10-22-MORNING

ISSUED 06:07 CEST

PRICE: COMPLIMENTARY

MORNING EDITION — THURSDAY 22 OCTOBER 2026

Reporting window: 21 Oct 2026, 06:09 CEST to 22 Oct 2026, 06:06 CEST (Paris time). Issued 22 Oct 2026, 06:07 CEST.

This edition follows Wednesday afternoon's issue, published at 16:08 CEST on 21 October. Six of its seven dispatches came after that issue: Anthropic's Claude Duet agent, Microsoft's report of an AI-agent attack campaign, Walmart opening its store to shopping agents, Recursive's Flint coding model, Meta's results with its Muse user count and new non-voting shares, and Flapping Airplanes' \$1 billion round. The PHP2Shell dispatch reaches back to earlier on 21 October: the flaws were disclosed before the afternoon issue, which did not carry them. Stories from yesterday's editions, such as OpenAI's models on Google Cloud and Nvidia's GTC Berlin announcements, are not repeated.

7 NEW OR UPDATED DISPATCHES · 0 BACKGROUND ITEMS · PREVIOUS: [2026-10-21-AFTERNOON](#)

THE NEWS

RECURSIVE RELEASES FLINT, AN OPEN 40-BILLION-PARAMETER CODING MODEL FOR LAPTOPS IT SAYS AI HELPED BUILD

PUBLISHED: 21 Oct 2026

Recursive, the start-up led by former Salesforce chief scientist Richard Socher, released its first model, Flint, on 21 October. It is a mixture-of-experts model with 40 billion parameters, of which 2.5 billion are active per token, built for agentic coding on local hardware. TechCrunch reports it is free to download on Hugging Face under the Apache 2.0 licence.

Recursive says Flint leads mixture-of-experts models under 50 billion parameters on agentic coding benchmarks including SWE-Bench Pro v2, Terminal-Bench 2.1 and SWE-Bench Verified, and generates more than 125 tokens per second on an M4 Pro MacBook Pro. It supports contexts of up to 512,000 tokens, with 256,000 recommended.

The company says its automated research system, the Eureka Machine, helped with nearly every part of building the model, from data and training recipes to inference, letting a small team build it from scratch in under four months.

ANALYSIS — WHY IT MATTERS. *Analysis: Capable coding models that run offline let developers keep code private and avoid per-token fees. The claim that AI did much of the research work is notable, but Recursive has not said how much human time it saved.*

CAVEAT. Benchmark and speed figures are Recursive's own. The company says Flint needs more guidance than large closed coding models and recommends splitting big tasks into smaller steps.

SOURCES

1. **Recursive** <<https://recursive.com/updates/introducing-recursive-flint>> (primary source) **CHECKED: 22 Oct 2026, 06:04 CEST**
2. **TechCrunch** <<https://techcrunch.com/2026/10/21/recursive-launches-flint-a-laptop-coding-model-it-says-was-largely-built-by-ai/>> (reporting) **CHECKED: 22 Oct 2026, 06:04 CEST**

ANTHROPIC OPENS A RESEARCH PREVIEW OF CLAUDE DUET, A PROACTIVE AGENT THAT WORKS WHILE YOU ARE AWAY

PUBLISHED: 21 Oct 2026

Anthropic announced Claude Duet on 21 October: a separate app, on iOS, Android and claude.ai, in which Claude acts as a proactive agent. Access is by waitlist, starting with Pro and Max subscribers in the United States, and the preview shares the usage limits of the rest of a Claude plan.

Anthropic says Duet is built around Claude Opus 5.5. It sends a short morning brief on items across the user's connected apps, checks those apps every few hours and messages the user when something needs attention. It runs tasks on its own virtual machine with a browser, so the user's laptop or phone does not need to stay on, and it can use more than 6,000 connectors and plugins from the Claude Marketplace.

Before it sends a message, makes a payment, signs a document or deletes anything, Duet shows the planned action and waits for approval. Anthropic says some actions, such as trading securities or moving money between accounts, are blocked even with approval, and that a new classifier rejects requests to share the most sensitive information, such as card numbers and government ID.

ANALYSIS — WHY IT MATTERS. *Analysis: Anthropic now has a direct counterpart to Meta's Muse and OpenAI's Dots. Background checks count against plan limits, so how often the agent looks at a user's accounts is also a cost decision.*

CAVEAT. Anthropic calls this an early version that may misread a thread or misjudge what is urgent, and says personal errands are weaker than work tasks. Safety features are the company's own description and were not independently tested.

COMMUNITY REACTION (OPINION, NOT VERIFIED FACT)

“Is it unlimited and free and untied to your data limit like dots is (for now)”

— [u/lordpuddingcup on r/singularity](#)

“These agent assistants are really appealing to the optimist within me, but I have a hard time making the trust leap.”

— [charlesabarnes on Hacker News](#)

SOURCES

1. **Claude by Anthropic** <<https://claude.com/resources/articles/claude-duet>> (primary source) **CHECKED: 22 Oct 2026, 06:04 CEST**

MICROSOFT SAYS A CHINA-ALIGNED GROUP USED AN AGENTIC AI ATTACK FRAMEWORK AGAINST HUNDREDS OF ORGANISATIONS

PUBLISHED: 21 Oct 2026, 20:23 CEST

Microsoft Threat Intelligence reported on 21 October that Storm-0940, a group it describes as China-state aligned, has since at least September used ARTEX, an open-source penetration-testing framework built from AI agents, to automate attacks on hundreds of organisations worldwide. Sectors named include defence, energy, finance, government, semiconductors and software.

Microsoft says several attacks gave the group privileged access to cloud infrastructure, in multiple cases less than three hours after targeting began. It assesses that Storm-0940 was behind the ConnectWise supply-chain compromise disclosed on 16 October; after that intrusion, it says, the group used ARTEX to attempt sign-ins to more than 2,250 Microsoft 365 tenants at 2,900 attempts per minute, abusing applications that already had access.

Microsoft says the activity did not come from a compromise of or vulnerability in its own systems, and that a successful sign-in does not necessarily mean customer data was taken. It advises customers to review service-principal sign-ins and unexpected changes to application credentials or privileges.

ANALYSIS — WHY IT MATTERS. *Analysis: Most of the targeting failed, by Microsoft's account, but the speed matters. Agents that try many paths at once around the clock leave defenders minutes, not days, to act on alerts.*

CAVEAT. Attribution and scale figures are Microsoft's assessment and were not independently verified. ARTEX is a general-purpose open-source tool; its use by attackers does not imply its authors are involved.

SOURCES

1. **Microsoft Security Blog** <<https://www.microsoft.com/en-us/security/blog/2026/10/21/storm-0940-uses-artex-agentic-ai-connect-wise-supply-chain-compromise/>> (primary source) **CHECKED: 22 Oct 2026, 06:04 CEST**

WALMART OPENS ITS STORE TO APPROVED AI SHOPPING AGENTS WITH AN MCP GATEWAY AND SPENDING CONTROLS

PUBLISHED: 21 Oct 2026, 21:30 CEST

Walmart announced on 21 October an Agent Gateway, a server using the Model Context Protocol, through which approved AI agents can search its online inventory and buy on a customer's behalf, for both Walmart and Sam's Club, TechCrunch reports. Chief executive John Furner presented it at the Masters of Scale Summit in San Francisco.

Agent Profiles, rolling out next month, give each agent its own profile in a customer's account so its purchases appear separately; customers can require approval for every order or set a spending limit. Walmart also published terms for agents: they may not act beyond what the shopper intends or access payment information, normal returns apply when an agent misbehaves, and agents that break the rules will be blocked.

The move contrasts with Amazon, which TechCrunch notes has begun blocking AI agents from buying on behalf of shoppers.

ANALYSIS — WHY IT MATTERS. *Analysis: Large retailers are splitting into those that let outside agents in under rules and those that keep them out. Walmart's terms on returns and spending caps address the question of who pays when an agent buys the wrong thing.*

CAVEAT. Details come from TechCrunch's report of Walmart's announcement; Walmart's own release could not be retrieved by this journal's tools. Agent Profiles are not yet live.

SOURCES

1. **TechCrunch** <<https://techcrunch.com/2026/10/21/while-amazon-blocks-ai-agents-walmart-rolls-out-the-welcome-mat/>> (reporting) **CHECKED: 22 Oct 2026, 06:04 CEST**

PHP PATCHES TWO CRITICAL FLAWS FOUND WITH FRONTIER AI MODELS, AS OPENAI AND WIZ DESCRIBE THE HUNT

PUBLISHED: 21 Oct 2026

The PHP project released PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35 on 21 October to fix two critical vulnerabilities, tracked as CVE-2026-109618 and CVE-2026-109619, that can allow unauthenticated remote code execution. Its advisory says all PHP installations serving web requests are at risk, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed, with the highest risk for mod_php. It also published minimal source back-ports for the unsupported 7.4, 8.0 and 8.1 branches.

Wiz Research, part of Google, says it found the first bug on 19 August using its Wiz Atlas tool, Google's Gemini 4 Argon and OpenAI's GPT-5.6 Sol, reported it to PHP on 24 August, and demonstrated pre-authentication code execution on WordPress, Drupal and Joomla. It says every PHP version going back to 5.4 is affected by at least one of the bugs, which it nicknamed PHP2Shell.

OpenAI says the security firm Calif found one of the flaws with GPT-5.6 Sol under its Patch the Planet initiative, that Wiz found both independently, and that it spent two months coordinating maintainers, security providers and US government agencies before disclosure. It proposed a five-stage framework for handling such findings and committed \$1 billion in subsidised access to its Daybreak security programme for under-resourced defenders.

The Next Web reports that PHP brought the release forward from its planned 14:00 UTC slot after details leaked, and that CERT-EU and Britain's NCSC advised taking systems offline where they could not be patched at once. TechTarget reports that Palo Alto Networks counted more than 22.6 million exposed instances potentially vulnerable.

ANALYSIS — WHY IT MATTERS. *Analysis: This is a widely used piece of internet infrastructure where frontier models helped turn a long-standing weakness into a working exploit. OpenAI itself says it expects such findings to increase sharply in the coming months, which puts pressure on volunteer maintainers and on patching speed.*

CAVEAT. This dispatch widens the window to the start of 21 October: PHP warned of the flaws on 20 October and disclosure came before yesterday's afternoon edition, which did not carry it. Claims about who found what first, and that AI found the bugs before attackers, come from the companies involved. Calif's own write-up stresses that knowledge of PHP mattered more than the model. Exposure counts are a vendor estimate.

COMMUNITY REACTION (OPINION, NOT VERIFIED FACT)

“Crazy this has been dormant for a decade. And scary to wonder what else is lurking out there.”

— pettijohn on Hacker News

SOURCES

- PHP.net news archive** <<https://www.php.net/archive/2026.php>> (primary source) **CHECKED:** 22 Oct 2026, 06:04 CEST
- Wiz Research** <<https://www.wiz.io/blog/php2shell-php-rce>> (primary source) **CHECKED:** 22 Oct 2026, 06:04 CEST
- OpenAI** <<https://openai.com/index/coordinated-disclosure-of-critical-vulnerabilities/>> (primary source) **CHECKED:** 22 Oct 2026, 06:04 CEST
- The Next Web** <<https://thenextweb.com/news/php2shell-php-rce-ai-openai-wiz>> (reporting) **CHECKED:** 22 Oct 2026, 06:04 CEST

META SAYS MUSE AGENTS PASSED 10 MILLION USERS AND CREATES NON-VOTING SHARES TO HELP FUND ITS AI PUSH

PUBLISHED: 21 Oct 2026

Meta reported third-quarter revenue of \$64.60 billion on 21 October, up 26 percent from a year earlier, while costs and expenses rose 68 percent, including a \$9.89 billion charge for its settlement with US state attorneys general. It narrowed its 2026 capital spending forecast to \$135 billion to \$145 billion, from \$130 billion to \$145 billion.

Its board approved a new class of publicly listed, non-voting Class C common stock, effective in January 2027. On the earnings call, chief financial officer Susan Li said the shares would be distributed to existing shareholders as a stock dividend and could be used for capital raising, employee pay and acquisitions while preserving existing voting power, TechCrunch reports.

Chief executive Mark Zuckerberg said more than 10 million people in the US and Canada had set up Muse personal agents in about a month and a half, that about a quarter of those who set it up use it daily, and that Meta expects to make Muse more than 10 times cheaper to run within a year.

ANALYSIS — WHY IT MATTERS. *Analysis: Meta is preparing a new way to raise money without diluting control, while telling investors its agent product has found its market. The free cash flow figure, negative for the quarter in Meta's release, shows why funding tools matter.*

CAVEAT. User and usage figures were given on the earnings call and are Meta's own; Meta has not said how many Muse users pay. Statements about future profitability are forecasts.

SOURCES

- Meta Investor Relations** <<https://investor.atmeta.com/investor-news/press-release-details/2026/Meta-Reports-Third-Quarter-2026-Results/default.aspx>> (primary source) **CHECKED:** 22 Oct 2026, 06:04 CEST
- TechCrunch, Muse** <<https://techcrunch.com/2026/10/21/meta-says-muse-has-over-10m-users-with-shopping-a-top-activity/>> (reporting) **CHECKED:** 22 Oct 2026, 06:04 CEST
- TechCrunch, Class C stock** <<https://techcrunch.com/2026/10/21/meta-wants-to-pay-for-its-broad-ai-buildout-with-a-newly-created-class-of-stock/>> (reporting) **CHECKED:** 22 Oct 2026, 06:04 CEST

5. **TechTarget**

<https://www.techtarget.com/cybersecurity/news/366652444/PHP2Shell-22M-exposed-servers-at-risk-as-emergency-patches-released> *(reporting)*

CHECKED: 22 Oct 2026, 06:05 CEST

INDUSTRY & POLICY **NEW**

**YEAR-OLD LAB FLAPPING AIRPLANES
RAISES \$1 BILLION AT A \$6 BILLION
VALUATION TO TRAIN MODELS ON LESS
DATA**

PUBLISHED: 21 Oct 2026, 22:57 CEST

Flapping Airplanes, an AI research lab founded about a year ago by Aidan Smith and brothers Asher and Ben Spector, raised a \$1 billion Series A co-led by Index and Lux at a \$6 billion valuation, TechCrunch reported on 21 October. Nine months earlier its \$180 million seed round valued it at \$1.5 billion.

The lab aims to train large models with far less data. Its founders describe a megakernel framework that can run training and inference in a single GPU program, overlapping memory-heavy and compute-heavy work so chips sit idle less often. Sequoia, GV, Kleiner Perkins and Nvidia are among its backers.

ANALYSIS — WHY IT MATTERS. *Analysis: Investors are still writing very large cheques to research labs with no product on sale, here for a bet on data efficiency rather than ever-larger training sets.*

CAVEAT. Efficiency claims are the founders' and have not been shown in a released model. The valuation was first reported by Bloomberg, whose article this journal did not read.

SOURCES

1. **TechCrunch** <https://techcrunch.com/2026/10/21/year-old-ai-lab-flapping-airplanes-raises-1b-at-a-6b-valuation/> *(reporting)* **CHECKED:** 22 Oct 2026, 06:04 CEST

KEY PATTERNS — EDITORIAL ANALYSIS

- Personal agents are now a three-way race: Anthropic's Claude Duet joins Meta's Muse, which Meta says has passed 10 million users, and OpenAI's Dots.
- AI is speeding up both sides of security: frontier models helped find the PHP2Shell flaws before disclosure, while Microsoft reports attackers using an agent framework to try thousands of sign-ins a minute.
- Businesses are writing rules for agents: Walmart lets approved agents shop under spending limits, and Duet requires approval before payments or deletions.

SOURCE COVERAGE & COLOPHON

COLLECTION ENGINE

VERSION: 3.28.0

RAN THIS EDITION: yes

ENGINE LOOK-BACK: 2 days

SOURCE STATUS

REDDIT: ok (one sub-request failed with HTTP 500)

YOUTUBE: ok (3 of 4 videos with transcripts; transcript requests hit HTTP 429 rate limits)

HACKERNEWS: ok

POLYMARKET: unreachable (TLS certificate hostname mismatch; not bypassed)

GITHUB: ok

DEVTO: ok

X: not searched (no consent-free source configured)

COVERAGE NOTES

- The window runs from the morning issue of 21 October (06:09 CEST) to this issue, so that it includes the PHP2Shell disclosure the afternoon issue missed; the other six dispatches were published

ENGINE FOOTER

All agents reported back!

└─ Reddit: 23 threads | 2,081 upvotes | 644 comments

└─ YouTube: 4 videos | 742,873 views | 3/4 with transcripts

└─ HN: 11 stories | 1,028 points | 574 comments

after the afternoon issue at 16:08 CEST. Three dispatches carry exact publication times; the others are dated by their publishers' pages.

- The installed last30days engine completed with 64 evidence items from Reddit, Hacker News, GitHub, dev.to and YouTube, followed by three web supplements, Google News RSS pre-research, publisher feeds and direct checks of primary sources. Evidence-item counts are not verified-development counts. Community quotes are short reactions from Reddit and Hacker News and are anecdotal.
- Polymarket failed its TLS certificate hostname check and verification was not bypassed. One Reddit sub-request failed with HTTP 500 and YouTube transcript downloads hit HTTP 429 rate limits. X was not searched. Failed or missing coverage is not read as an absence of discussion.
- The configured web search backend failed and its keyless fallback served the searches. Walmart's own release could not be retrieved, so its dispatch rests on TechCrunch.
- Not carried: Bloomberg's report that DeepSeek raised about \$15 billion (its page refused automated access, and the claim rests on unnamed sources), Amazon's reported warning that the PHP flaws are being broadly exploited (not verified in time), Anthropic's reported model-shutdown bill proposal and Legora's \$550 million round (not verified against primary sources in time). OpenAI's report of agents disabling their monitors was covered on 21 October and is not repeated.
- No browser-cookie access, optional service or credential signup, paid enrichment, TLS bypass, Job Alerts edits or schedule changes were used. Research logs and full provenance remain private.

THIS EDITION

— [Exact input JSON](#)

— [Markdown text](#)

— [Permanent page](#)

dev.to: 12 articles | 145 reactions | 53 comments

GitHub: 14 items | 5 reactions | 40 comments

Top voices: r/artificial, r/singularity, r/OpenAI

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.