

The US Gazette

Models, machines, and matters of consequence

PARIS, THURSDAY 22 OCTOBER 2026 AFTERNOON EDITION · No. 2026-10-22-AFTERNOON ISSUED 16:08 CEST PRICE: COMPLIMENTARY

AFTERNOON EDITION — THURSDAY 22 OCTOBER 2026

Reporting window: 21 Oct 2026, 06:09 CEST to 22 Oct 2026, 16:07 CEST (Paris time). Issued 22 Oct 2026, 16:08 CEST.

This edition follows this morning's issue, published at 06:07 CEST. Six of its seven dispatches were published after it: 1Password's sign-in system for personal agents, a report that US banks are blocking unvetted agents, Google's Agent Compute Engine, Hugging Face's Carbon-X DNA model, Barclays' AI-linked job cuts, and DeepSeek's reported \$15 billion round, which the morning issue could not yet verify. The LiteLLM dispatch reaches back to 21 October: the compromised release was pulled that afternoon and neither of the two previous editions carried it. Stories from the morning edition, such as Claude Duet, the PHP flaws and Meta's results, are not repeated.

7 NEW OR UPDATED DISPATCHES · 0 BACKGROUND ITEMS · PREVIOUS: [2026-10-22-MORNING](#)

THE NEWS

HUGGING FACE RELEASES CARBON-X, AN OPEN 14.8-BILLION-PARAMETER MODEL THAT READS AND WRITES DNA IN PLAIN-LANGUAGE CHAT

PUBLISHED: 22 Oct 2026, 12:00 CEST

Hugging Face released Carbon-X on 22 October, an open model under the Apache 2.0 licence, built with Zhongguancun Academy and the Telethon Institute of Genetics and Medicine at the University of Naples Federico II. Its model card describes a 14.8-billion-parameter model, trained from Qwen3-14B on DNA sequences and ordinary text, that takes raw DNA inside a chat and answers in English, for example predicting whether a mutation is likely to be harmful.

Hugging Face reports that across five DNA benchmarks, covering variant-effect prediction, sequence understanding and next-base prediction, Carbon-X averages 66.7% with reasoning turned off: 27 points above the Qwen3-14B model it started from and ahead of the other open models it tested. Senior research scientist Lewis Tunstall told Business Insider the team wanted to give researchers tools that do not leave them dependent on a single external provider, and that viruses were left out of the training data to reduce the risk of misuse.

ANALYSIS — WHY IT MATTERS. *Analysis: Because it runs on a researcher's own hardware, labs can analyse sensitive genetic data without sending it to an outside AI company.*

CAVEAT. Benchmarks are Hugging Face's own selection and were not independently reproduced. The model card says Carbon-X has not been clinically validated and should not be used for medical decisions, and that quality drops on long generated sequences.

SOURCES

- Hugging Face model card**
<<https://huggingface.co/HuggingFaceBio/Carbon-X>> (primary source)
CHECKED: 22 Oct 2026, 16:04 CEST
- Business Insider** <<https://www.businessinsider.com/hugging-face-ai-model-carbon-x-dna-sequences-gene-therapies-2026-10>> (reporting)
CHECKED: 22 Oct 2026, 16:04 CEST

LITELLM'S 1.107.0 RELEASE SHIPPED A CREDENTIAL STEALER TO PYPI AND DOCKER, THE POPULAR AI GATEWAY'S SECOND COMPROMISE THIS YEAR

PUBLISHED: 21 Oct 2026

LiteLLM, an open-source Python library and proxy that lets developers call many AI model providers through one interface, says its release pipeline was compromised early on 21 October and pushed a malicious version 1.107.0 to PyPI and to its Docker images. LiteLLM says the PyPI wheels were live from 11:39 to 13:23 UTC, and that several of its Docker image tags pointed to compromised images from 11:46 UTC until they were taken down in the early afternoon.

According to the OSV malware record and LiteLLM's own notice, the malicious files were not in the project's source code: they were added at build or upload time. Each wheel installs three extra files at the root of site-packages, so the payload runs every time Python starts, even if LiteLLM is never imported. The record lists what it collects: cloud credentials for AWS, Google Cloud and Azure, SSH, GPG and TLS keys, Kubernetes, Docker and CI secrets, configuration files of AI coding tools, browser passwords and environment variables. A second component fetches and runs code from a remote server every hour.

LiteLLM says all earlier releases are safe, its private enterprise registry was not affected, and users should pin version 1.106.2. It advises treating any environment that started Python with 1.107.0 as compromised, rebuilding it rather than cleaning it, and rotating every credential the host could reach, including the provider keys stored in a LiteLLM proxy database. Datadog Security Labs puts the library at about 23 million weekly downloads and notes this is LiteLLM's second supply-chain compromise in 2026, after versions 1.82.7 and 1.82.8, an incident LiteLLM dates to March; Datadog says no link between the two incidents has been established.

ANALYSIS — WHY IT MATTERS. *Analysis: AI gateways hold the keys to many model providers at once, so a poisoned release can leak far more than one account. The payload also targeted the settings of AI coding tools, which increasingly hold their own credentials.*

CAVEAT. This dispatch reaches back before both of yesterday's later editions: the release was pulled on 21 October, and neither the afternoon nor the morning edition carried it. LiteLLM says its investigation is still in progress and has not published how the attacker obtained access. Download figures are Datadog's estimate.

COMMUNITY REACTION (OPINION, NOT VERIFIED FACT)

- “This... isn't acceptable. Once is forgivable, twice is malpractice.”
— [stbenjam](#) on Hacker News
- “Seriously again for litellm? I really with that things like Google ADK didn't add this to my deps.”
— [rleveng](#) on Hacker News

SOURCES

- LiteLLM security notice** <<https://docs.litellm.ai/blog/security-incident-oct-21-2026>> (primary source) **CHECKED: 22 Oct 2026, 16:04 CEST**
- OSV malware record MAL-2026-2144**
<<https://osv.dev/vulnerability/MAL-2026-2144>> (primary source)
CHECKED: 22 Oct 2026, 16:04 CEST
- BerriAI/litellm issue 47826**
<<https://github.com/BerriAI/litellm/issues/47826>> (primary source)
CHECKED: 22 Oct 2026, 16:06 CEST

1PASSWORD LETS MUSE, CLAUDE DUET, CHATGPT AND GROK AGENTS SIGN IN FOR USERS WITHOUT EVER SEEING THEIR PASSWORDS

PUBLISHED: 22 Oct 2026

1Password announced 1Password for Agents on 22 October, a sign-in system for personal AI agents. When an agent reaches a login page, it asks 1Password for a credential; the user is told which account the agent wants and why, and approves or refuses on their own device. If approved, 1Password fills the login into the page itself, so the password and one-time codes never reach the agent or the model behind it.

1Password names integrations with Meta's Muse, Anthropic's Claude Duet, OpenAI's ChatGPT Work and Dots, SpaceXSI's Grok Bot and Town, rolling out over the coming days, and says Instinct, Browserbase, Browser Use, Dana, Kernel, Perplexity, Ramp, Tomo and Wajo are coming. The Verge reports that access is approved per sign-in request rather than handed over permanently.

SiliconANGLE quotes Anthropic's chief product officer, Ami Vora, as saying 1Password will "soon" fill in Duet's sign-ins, so for Duet the integration is not yet live.

ANALYSIS — WHY IT MATTERS. *Analysis: Personal agents need logins to be useful, and pasting a password into a chat is the habit this replaces. It limits what an agent can learn; it does not stop an agent from making a wrong purchase once signed in.*

CAVEAT. Security claims are 1Password's own description and have not been independently tested. Partner timing varies, and some integrations are announced rather than available.

SOURCES

- 1Password** <<https://1password.com/blog/1password-for-ai-agents>> (primary source) **CHECKED: 22 Oct 2026, 16:05 CEST**
- The Verge** <<https://www.theverge.com/ai-artificial-intelligence/1016399/1password-ai-agent-password-sign-in>> (reporting) **CHECKED: 22 Oct 2026, 16:04 CEST**
- SiliconANGLE** <<https://siliconangle.com/2026/10/22/1password-for-agents-lets-personal-ai-agents-log-in-without-ever-seeing-the-password/>> (reporting) **CHECKED: 22 Oct 2026, 16:04 CEST**

GOOGLE TURNS THE COMPUTERS BEHIND GEMINI'S AGENTS INTO A CLOUD SERVICE AND OPEN-SOURCES A KUBERNETES VERSION

PUBLISHED: 22 Oct 2026

Google Cloud announced Agent Compute Engine on 22 October, a service that gives each AI agent its own hardware-isolated micro virtual machine. Google says the service already runs Gemini's agents for work tasks and will open to customers in preview in the coming months.

Google says idle agents are paused and resumed from snapshots, so a waiting agent uses almost no resources, and that the sandbox holds no long-lived credentials: an off-machine gateway checks each outbound request and adds the needed credential only after it leaves the sandbox. It also released Agent Substrate, an open-source runtime for Google Kubernetes Engine, which it says sustained 500 activations a second across 200,000 agents in its own benchmark.

The company is also extending its agent governance tools, including an agent registry, per-agent identities and a gateway with token budgets and model routing, to other clouds, on-premises systems and coding agents such as Claude Code on company devices, mostly in preview.

ANALYSIS — WHY IT MATTERS. *Analysis: Google is selling the same approach the banks and 1Password are reaching for: keep secrets away from the agent and check every action at a gateway. Performance and density figures are Google's own and come from its own tests.*

CAVEAT. Agent Compute Engine is not yet available to customers; Google gives no date beyond the coming months. Benchmark numbers are vendor claims.

SOURCES

- Google Cloud** <<https://cloud.google.com/blog/topics/ai-infrastructure/introducing-agent-compute-engine-and-expanded-agent-governance>> (primary source) **CHECKED: 22 Oct 2026, 16:04 CEST**
- Google Cloud technical deep dive** <<https://cloud.google.com/blog/topics/ai-infrastructure/agent-compute-engine-deep-dive>> (primary source) **CHECKED: 22 Oct 2026, 16:05 CEST**
- The New Stack** <<https://thenewstack.io/google-agent-compute-engine/>> (reporting) **CHECKED: 22 Oct 2026, 16:06 CEST**

4. Datadog Security Labs

<<https://securitylabs.datadoghq.com/articles/litellm-compromised-pypi-docker/>> (reporting) **CHECKED: 22 Oct 2026, 16:04 CEST**

DEEPSEEK IS REPORTED TO HAVE RAISED ABOUT \$15 BILLION FROM TENCENT, CATL AND OTHER CHINESE BACKERS AHEAD OF A POSSIBLE LISTING

PUBLISHED: 22 Oct 2026, 08:20 CEST

Bloomberg reported on Thursday, citing unnamed people familiar with the matter, that the Chinese AI developer DeepSeek has raised about 100 billion yuan (about \$15 billion) in its latest round, one of the largest ever for a Chinese company. It says DeepSeek raised its target at least twice, from 50 billion yuan to 80 billion yuan before reaching the final figure, and that the battery maker CATL and Tencent were among the biggest investors.

Reuters, citing four people with knowledge of the matter, reported the same total and named more backers: new investors including the chipmaker GigaDevice, Meituan, Geely and Midea, alongside existing shareholders NetEase and IDG Capital, with more than 15 investors in all. Reuters says sources have put DeepSeek's value at 500 billion yuan before the new money, and that the round should close in the coming days but its details could still change.

Both outlets tie the round to a possible stock market listing. Reuters had reported in September that DeepSeek hired CITIC Securities for a potential float on Shanghai's STAR Market. DeepSeek did not respond to either outlet.

ANALYSIS — WHY IT MATTERS. *Analysis: The round narrows, but does not close, the funding gap with US labs; Bloomberg notes Anthropic and OpenAI have each raised more than \$100 billion. A shareholder list made of Chinese chip, battery, car and internet companies ties DeepSeek more closely to China's domestic supply chain.*

CAVEAT. Not confirmed by DeepSeek. All figures come from unnamed sources, and Reuters says the investor list and terms are not final. The morning edition left this out because Bloomberg's original report could not be read in full; this edition relies on Bloomberg's text as republished by Mint and on Reuters' separate reporting.

SOURCES

- Bloomberg via Mint** <<https://www.livemint.com/companies/news/deepseek-raises-15-billion-to-challenge-anthropic-openai-and-other-us-ai-labs-11792649782182.html>> (reporting) **CHECKED: 22 Oct 2026, 16:05 CEST**
- Reuters via KSL** <<https://www.ksl.com/article/51639460/deepseek-wrapping-up-15-billion-fundraising-to-fuel-ai-race>> (reporting) **CHECKED: 22 Oct 2026, 16:04 CEST**

AXIOS: MAJOR US BANKS ARE FINDING UNVETTED AI AGENTS INSIDE CUSTOMER ACCOUNTS AND ARE MOVING TO BLOCK THEM

PUBLISHED: 22 Oct 2026

Axios reported on 22 October, citing people familiar with the issue, that major US banks are detecting third-party AI agents operating inside customer accounts, in some cases trying to take actions that appeared independent of the user's instructions. Most cases involve agents logging in with the customer's own permission and password, which still breaks most banks' rules that customers log in themselves.

According to Axios, Morgan Stanley has begun blocking third-party agents, and JPMorgan, Bank of America and Citi are also restricting them. A Chase spokesperson said customers should not share their usernames and passwords with anyone; a Morgan Stanley spokesperson said the bank had not seen "rogue AI agents accessing our platforms." Axios says most banks are allowing, or moving towards, read-only access for agents, and that some cannot tell whether account activity was directed by the user.

ANALYSIS — WHY IT MATTERS. *Analysis: Read-only access for agents looks like the banks' near-term compromise, which leaves agents able to see finances but not move money. It is the same problem 1Password and Walmart are trying to solve with approval steps.*

CAVEAT. This rests on Axios' unnamed sources; Reuters, which relayed the report, said it could not immediately verify it. Axios blocked direct automated access, so the text was read through the configured search tool's extract.

SOURCES

- Axios** <<https://www.axios.com/2026/10/22/ai-agents-banks-unauthorized-accounts-access>> (reporting) **CHECKED: 22 Oct 2026, 16:06 CEST**

BARCLAYS IS CUTTING ABOUT 5,000 JOBS, AROUND 5% OF ITS STAFF, AS IT USES MORE AI

PUBLISHED: 22 Oct 2026, 10:00 CEST

Bareclays said on 22 October that it is cutting about 5,000 jobs, around 5% of its global workforce, as it brings more AI into its work, the BBC reported. About 1,000 posts have already gone and the other 4,000 are expected to go by the end of the year. Around 60% of the cuts fall in support functions, including among developers, and a large share are expected in India, where some UK back-office work is done.

The bank said not all the cuts are due to AI and that they are part of a longer modernisation plan. Chief executive C.S. Venkatakrishnan said: "AI is the icing on the cake not the cake." Bareclays expects its efficiency measures to save a further 1.1 billion pounds in 2027, and reported a 2.3 billion pound quarterly profit.

ANALYSIS — WHY IT MATTERS. *Analysis: A large bank is now putting a number on AI-linked job cuts, and developers are among the roles affected. HSBC, Standard Chartered and Danske Bank have also flagged AI-related cuts this year, the BBC notes.*

CAVEAT. Bareclays does not say how many of the 5,000 jobs are cut because of AI rather than its wider cost programme.

SOURCES

- BBC News** <<https://www.bbc.com/news/articles/cm4g1p347qgxo>> (reporting) **CHECKED: 22 Oct 2026, 16:04 CEST**
- CNBC** <<https://www.cnbc.com/2026/10/22/barclays-ai-jobs-cuts.html>> (reporting) **CHECKED: 22 Oct 2026, 16:04 CEST**

KEY PATTERNS — EDITORIAL ANALYSIS

- Agent access is the theme of the day: 1Password and Google both keep credentials out of the agent's reach, while US banks are reported to be blocking agents that log in with customers' passwords.
- AI developer tooling is now a target in its own right: the poisoned LiteLLM release went after cloud keys, model-provider keys and AI coding tool settings.
- Money keeps flowing to AI and away from staff: DeepSeek's reported \$15 billion round and Bareclays' 5,000 job cuts landed on the same day.

SOURCE COVERAGE & COLOPHON

COLLECTION ENGINE

VERSION: 3.28.0
RAN THIS EDITION: yes
ENGINE LOOK-BACK: 2 days

SOURCE STATUS

REDDIT: ok
YOUTUBE: ok (1 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 LiteLLM compromise that both previous editions missed; the other six dispatches were published after this morning's issue at 06:07 CEST. Three dispatches carry exact publication times; the others are dated by their publishers' pages.
- The installed last30days engine completed with 69 evidence items from Reddit, Hacker News, GitHub, dev.to and YouTube, followed by three web supplements, Google News RSS pre-research and di-

ENGINE FOOTER

All agents reported back!
└─ Reddit: 17 threads | 1,448 upvotes | 372 comments
└─ YouTube: 4 videos | 457,500 views | 1/4 with transcripts
└─ HN: 12 stories | 2,960 points | 1,105 comments
└─ dev.to: 12 articles | 145 reactions | 89 comments
└─ GitHub: 24 items | 15 reactions | 218 comments
└─ Top voices: r/artificial, r/singularity, r/OpenAI

- rect checks of primary sources. Evidence-item counts are not verified-development counts. Community quotes are short reactions from Hacker News and are anecdotal.
- Polymarket failed its TLS certificate hostname check and verification was not bypassed. 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. Axios, Business Wire and several Reuters syndication pages refused automated access; the banks dispatch rests on Axios text read through the search tool.
 - Not carried: Yahoo Finance's report that Anthropic could publicly file its IPO prospectus as early as Friday (a date that rests on unnamed sources and has not happened), DeepSeek's DeepInfer serving framework and the US ban on DeepSeek in federal agencies (both dated 20 October, before this window), and general AI market moves.
 - 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](#)

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.