The AJ Gazette

Models, machines, and matters of consequence

Paris, Friday 30 October 2026 · Afternoon edition · No. 2026-10-30-afternoon · Issued 16:08 CET · Price: Complimentary

AFTERNOON EDITION — FRIDAY 30 OCTOBER 2026

Reporting window: 29 Oct 2026, 16:07 CET to 30 Oct 2026, 16:07 CET (Paris time). Issued 30 Oct 2026, 16:08 CET.

This edition has six new stories and no repeats of this morning's issue. Two of them, a backdoored Claude Code extension in Cursor's marketplace and Epoch AI's Firefox exploit study, are dated 29 October but were missed this morning, so the window reaches back to yesterday's 16:07 issue. The rest are from today: an AI-spending selloff led by Intel, Wikimedia's brief in the New York Times case, Foxconn's planned OpenAI deal and Apple's purchase of Ascend.io.

6 new or updated dispatches · 0 background items · Previous: 2026-10-30-morning

THE NEWS

Coding & agents NEW

CURSOR SAYS A TAMPERED CLAUDE CODE EXTENSION IN ITS MARKETPLACE PLANTED AN SSH BACKDOOR ON UP TO 5,000 MACHINES

Published: 29 Oct 2026

Cursor, the AI coding editor owned by SpaceX, published a security notice dated 29 October. It says a maliciously modified Anthropic.claude-code version 2.1.313 was available in its own VS Code extension marketplace from about 2:27am to 1:35pm Pacific time that day. Cursor says the version was not developed by Anthropic and that at most 5,000 users were affected; it will contact them directly.

According to Cursor, the code collects host and user details, adds an attacker's SSH key labelled svc-telemetry to the user's authorized keys, installs persistence and tries to open a reverse SSH tunnel. Cursor says turning on the SSH service fails on most macOS and Windows machines because it needs administrator rights, but the key, the persistence and the host report still go through. Uninstalling the extension may not be enough, it says, and it publishes a check and removal scripts.

Cursor says it removed the version, shut down and rebuilt the marketplace, rotated its keys, audited access and found no other tampered extensions, and had the attacker's server taken offline. The Hacker News reports that the package was shipped under the extension's legitimate ID, that there is no evidence it reached Open VSX or Microsoft's marketplace, and that Anthropic has published version 2.1.314 to both.

Analysis — why it matters. *Analysis: AI coding agents run with the developer's own permissions, so a poisoned update to one of them is a direct route into source code and credentials. Here the weak point was a third-party marketplace, not the vendor's own release.*

Caveat. How the attacker got the package into Cursor's marketplace has not been explained, and no statement from Anthropic was found. The 5,000 figure is Cursor's upper bound.

Community reaction (opinion, not verified fact)

> "How will they communicate and fix that."
>
> — mrweasel (Hacker News)

> "Is this affecting only people using Cursor or all VS Code users?"
>
> — ale42 (Hacker News)

Sources

1. **Cursor: security notice** <https://cursor.com/blog/claude-code-extension-security-notice> *(primary source)* ***Checked:*** *30 Oct 2026, 16:04 CET*
2. **The Verge** <https://www.theverge.com/ai-artificial-intelligence/1023096/cursor-says-around-5000-people-may-have-installed-a-malicious-claude-code-extension> *(reporting)* ***Checked:*** *30 Oct 2026, 16:04 CET*
3. **The Hacker News** <https://thehackernews.com/2026/10/official-claude-code-vs-code-extension.html> *(reporting)* ***Checked:*** *30 Oct 2026, 16:04 CET*
4. **Phorion: technical advisory** <https://phorion.io/blog/offical-claude-code-vsx-compromise/> *(reporting)* ***Checked:*** *30 Oct 2026, 16:04 CET*
5. **Hacker News discussion** <https://news.ycombinator.com/item?id=50300683> *(community)* ***Checked:*** *30 Oct 2026, 16:06 CET*

Research NEW

EPOCH AI: THE OPEN-WEIGHT MODEL GLM 5.3 BUILT WORKING FIREFOX EXPLOITS FROM SECURITY FIXES BEFORE USERS RECEIVED THEM

Published: 29 Oct 2026

Epoch AI published a report on 29 October on the patch gap, the time between a security fix appearing in public code and reaching users. Its researchers say Z.ai's open-weight model GLM 5.3 built webpages that read a file from a visitor's computer and sent it to an attacker, against all six Firefox releases from 17 September to 26 October.

The researchers say they ran the model offline with basic tools and public information from each release date, and that it worked without human input after basic instructions. Once their setup was built, each version cost about $1,000 in API fees; the fastest attempt took 12 hours. They say no provider, including Z.ai, refused the requests. Each attack also used an unpublished sandbox flaw that the model rediscovered; Firefox 159.0, released on 27 October, patches it.

The same approach did not produce a Chrome exploit. In a post on 29 October, Mozilla said it now ships builds every week, keeps regression tests confidential until fixes ship, scans new commits, and will time fixes so that the pieces an attacker must chain are never in the patch gap at the same time.

Analysis — why it matters. *Analysis: Offensive skills once reserved for tightly held frontier models are showing up in freely available ones, which shifts the defence towards how quickly and quietly fixes ship.*

Caveat. This is Epoch AI's own experiment, not peer reviewed. The team spent more than $100,000 building and testing the setup, and has not confirmed whether the attack works on Firefox 159.0.

Sources

1. **Epoch AI: report** <https://epoch.ai/publications/open-weight-models-patch-gap> *(primary source)* ***Checked:*** *30 Oct 2026, 16:05 CET*
2. **Mozilla: Defending the patch gap** <https://blog.mozilla.org/en/firefox/privacy-security/defending-patch-gap/> *(primary source)* ***Checked:*** *30 Oct 2026, 16:05 CET*
3. **The Decoder** <https://the-decoder.com/open-weight-model-glm-5-3-built-full-firefox-exploit-chains-with-zero-human-input-in-under-48-hours/> *(reporting)* ***Checked:*** *30 Oct 2026, 16:04 CET*

Industry & policy NEW

INTEL FALLS MORE THAN 30% AND DRAGS CHIP STOCKS DOWN AS THE SELLOFF OVER AI SPENDING REACHES THE NASDAQ

Published: 30 Oct 2026, 15:35 CET

US technology stocks fell sharply on Friday morning. Reuters reported that Intel fell more than 30%, on course for its biggest one-day loss on record, after warning that it would burn cash this year because of a weak PC market, manufacturing problems and heavy spending on production. Amazon slipped 2% after reporting its cash outflow the day before.

The selloff spread to chipmakers: Reuters reported Nvidia down 3%, AMD down 9.3% and the chips index down 5.7%, with Dell and HP down about 9%. At 09:53 New York time the Nasdaq Composite was down 2.21% and the S&P 500 down 1.22%. Reuters said the Nasdaq-100 was on track to erase just over $1 trillion in market value if losses held. Reddit fell 26% after warning that daily visitors could drop.

Intel's chief executive, Lip-Bu Tan, told investors he was disappointed not to meet strong customer demand, citing manufacturing, supply shortages and an unprecedented memory crunch, NBC News reported.

Analysis — why it matters. *Analysis: A week that started with questions about cloud giants' cash flow now reaches the suppliers; investors are pricing the cost of the AI build-out, not only its demand.*

Caveat. These are intraday figures from Friday morning in New York; closing prices were not available when this edition went to press.

Sources

1. **Reuters via Yahoo Finance** <https://finance.yahoo.com/markets/stocks/articles/nasdaq-futures-sink-amazon-intel-114737736.html> *(reporting)* ***Checked:*** *30 Oct 2026, 16:05 CET*
2. **NBC News** <https://www.nbcnews.com/business/markets/tech-stocks-nasdaq-ai-boom-fears-deepen-rcna606512> *(reporting)* ***Checked:*** *30 Oct 2026, 16:05 CET*

Industry & policy NEW

WIKIMEDIA ASKS THE COURT IN THE NEW YORK TIMES CASE AGAINST OPENAI TO TREAT AI TRAINING AS FAIR USE, BUT NOT CHATBOT RETRIEVAL

Published: 30 Oct 2026, 10:00 CET

The Wikimedia Foundation, which runs Wikipedia, said on 30 October that it had filed an amicus brief in In re: OpenAI, Inc. Copyright Infringement Litigation, the 12 combined lawsuits against OpenAI that include The New York Times' case against Microsoft and OpenAI, in the Southern District of New York. It says it supports neither side.

The foundation argues that using copyrighted works to train models that are new and different from their sources should count as fair use, without licensing terms. It argues that retrieval-augmented generation, where a chatbot copies web content to answer a question, should not count as fair use and must respect each publisher's licence; for Wikipedia that means CC BY-SA 4.0 attribution. It also says scraping of its sites must respect its rate limits or go through its paid Enterprise API.

Analysis — why it matters. *Analysis: The brief splits training from retrieval, the distinction that matters most for AI search products, and comes from the site whose content is among the most used to train and ground chatbots.*

Caveat. This is one party's legal argument, not a ruling. Unite.AI reports that the filing is a request for leave to file the brief, which the judge has not yet decided.

Sources

1. **Wikimedia Foundation** <https://wikimediafoundation.org/news/2026/10/30/wikimedia-foundation-amicus-brief-new-york-times-v-open-ai-case/> *(primary source)* ***Checked:*** *30 Oct 2026, 16:05 CET*
2. **The Verge** <https://www.theverge.com/policy/1022880/wikipedia-openai-new-york-times-copyright> *(reporting)* ***Checked:*** *30 Oct 2026, 16:05 CET*
3. **Unite.AI** <https://www.unite.ai/wikimedia-foundation-seeks-to-file-amicus-brief-in-openai-copyright-case/> *(reporting)* ***Checked:*** *30 Oct 2026, 16:08 CET*

Industry & policy NEW

FOXCONN SAYS A NEW COLLABORATION WITH OPENAI IS IN THE WORKS AFTER ITS CHAIRMAN MET SAM ALTMAN

Published: 30 Oct 2026, 09:38 CET

Foxconn chairman Young Liu told reporters at the company's annual technology event in Taipei on Friday that he had met OpenAI chief executive Sam Altman earlier that day, and that a new collaboration with OpenAI was in the works, Reuters reported. He said there would be an announcement once details were confirmed and gave no further details.

Reuters notes that any deal would build on last year's agreement for the two companies to design and engineer data-centre racks and other AI hardware. Liu also said the AI industry was not in a bubble and that Foxconn, Nvidia's biggest AI server maker, expects double-digit growth next year.

Analysis — why it matters. *Analysis: OpenAI keeps lining up hardware partners directly, alongside the chipmakers whose shares were falling on the same day.*

Caveat. No terms were given and OpenAI's comment was not found; the growth outlook is Foxconn's own.

Sources

1. **CNA (Reuters)** <https://www.channelnewsasia.com/business/foxconn-working-new-tie-up-openai-says-there-no-ai-bubble-6506396> *(reporting)* ***Checked:*** *30 Oct 2026, 16:04 CET*

Industry & policy NEW

APPLE'S EU DISCLOSURE SHOWS A DEAL FOR AGENTIC DATA-ENGINEERING STARTUP ASCEND.IO

Published: 30 Oct 2026, 13:06 CET

An update to the European Commission's list of acquisitions under the Digital Markets Act shows a deal between Apple and Ascension Labs, better known as Ascend.io, a company that sells AI agents for data engineering, 9to5Mac and MacRumors reported on 30 October.

According to the reports, Apple gets the right to make employment offers to certain employees, a non-exclusive licence to Ascend's intellectual property and some of its patents. Ascend's website says it is winding down operations.

Analysis — why it matters. *Analysis: Like other recent Apple deals, this is structured as a hiring and licensing deal rather than a classic takeover, which keeps it small.*

Caveat. The Commission's page was not read directly, and no price was disclosed.

Sources

1. **9to5Mac** <https://9to5mac.com/2026/10/30/apple-acquires-ascend%E2%80%A4io-an-agentic-ai-engineering-startup/> *(reporting)* ***Checked:*** *30 Oct 2026, 16:04 CET*
2. **MacRumors** <https://www.macrumors.com/2026/10/30/apple-acquires-ascend-io/> *(reporting)* ***Checked:*** *30 Oct 2026, 16:05 CET*
3. **AppleInsider** <https://appleinsider.com/articles/26/10/30/ai-data-handling-firm-ascendio-acquired-by-apple> *(reporting)* ***Checked:*** *30 Oct 2026, 16:08 CET*
4. **The Verge** <https://www.theverge.com/tech/1023069/apple-has-acquired-ai-data-engineering-startup-ascend-io> *(reporting)* ***Checked:*** *30 Oct 2026, 16:04 CET*

KEY PATTERNS — EDITORIAL ANALYSIS

— AI developer tools are now a supply-chain target: one poisoned extension update reached up to 5,000 machines in a day.
— Freely available models are closing in on offensive security work, and defenders are answering by shipping fixes faster and more quietly.
— Markets are pricing the cost of the AI build-out across the supply chain, from cloud giants to chipmakers such as Intel.

SOURCE COVERAGE & COLOPHON

COLLECTION ENGINE

Version: 3.28.0
Ran this edition: yes
Engine look-back: 2 days

SOURCE STATUS

reddit: ok (23 threads)
youtube: ok (4 videos, 2 with transcripts; other transcript requests hit HTTP 429)
hackernews: ok (14 stories)
polymarket: unreachable (TLS certificate hostname mismatch; not bypassed)
github: ok (21 items)
devto: searched with tags ai, machinelearning and llm; 0 articles returned
x: not searched (no consent-free source configured)

COVERAGE NOTES

— The window runs from yesterday's 16:07 CET issue to this edition, wider than usual, to carry two 29 October items that this morning's edition missed. Dispatches with only a date carry that date; exact timestamps are given where a source supplied one.
— The installed last30days engine finished with 62 evidence items from Reddit, Hacker News, GitHub and YouTube. Its top items were videos about the AI stock selloff and Hacker News threads on the Claude Code extension backdoor, which supplied the community

ENGINE FOOTER

All agents reported back!
├— Reddit: 23 threads | 826 upvotes | 684 comments
├— YouTube: 4 videos | 2,318,272 views | 2/4 with transcripts
├— HN: 14 stories | 1,839 points | 791 comments

quotes. Stories were chosen with Google News RSS, publisher feeds, web searches and checks of primary documents. Item counts are not counts of verified developments.

— Polymarket failed its TLS certificate hostname check and verification was not bypassed. X was not searched. dev.to returned no articles. YouTube transcript requests hit HTTP 429. Failed or missing coverage does not mean nobody discussed these stories.

— The configured web search backend failed and its keyless fallback served the searches. VentureBeat returned HTTP 429; Reuters copies on StreetInsider and the AP market report returned HTTP 403, so the market dispatch relies on Reuters' text on Yahoo Finance and on NBC News. The European Commission's acquisitions page and MLex were not read.

— Not carried: an AI audit of 138 economics papers (reported 28 October, before this window), DeepSeek's funding round (reported 22 October), Cognizant's OpenAI staffing pledge (a company announcement), and Gemini's in-chat document editing.

— 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

├─ GitHub: 21 items | 10 reactions | 16 comments
├─ Top voices: r/singularity, r/artificial, 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.