

SNOK

WEEKLY REVIEW W45

Faster than the patch

SNOK's review of 30 October - 5 November 2026: SAP flaws, agents in SAP and UiPath, supply-chain incidents, Linux, agentic attack tools, AI oversight, and the money and hardware behind AI

Swipe →

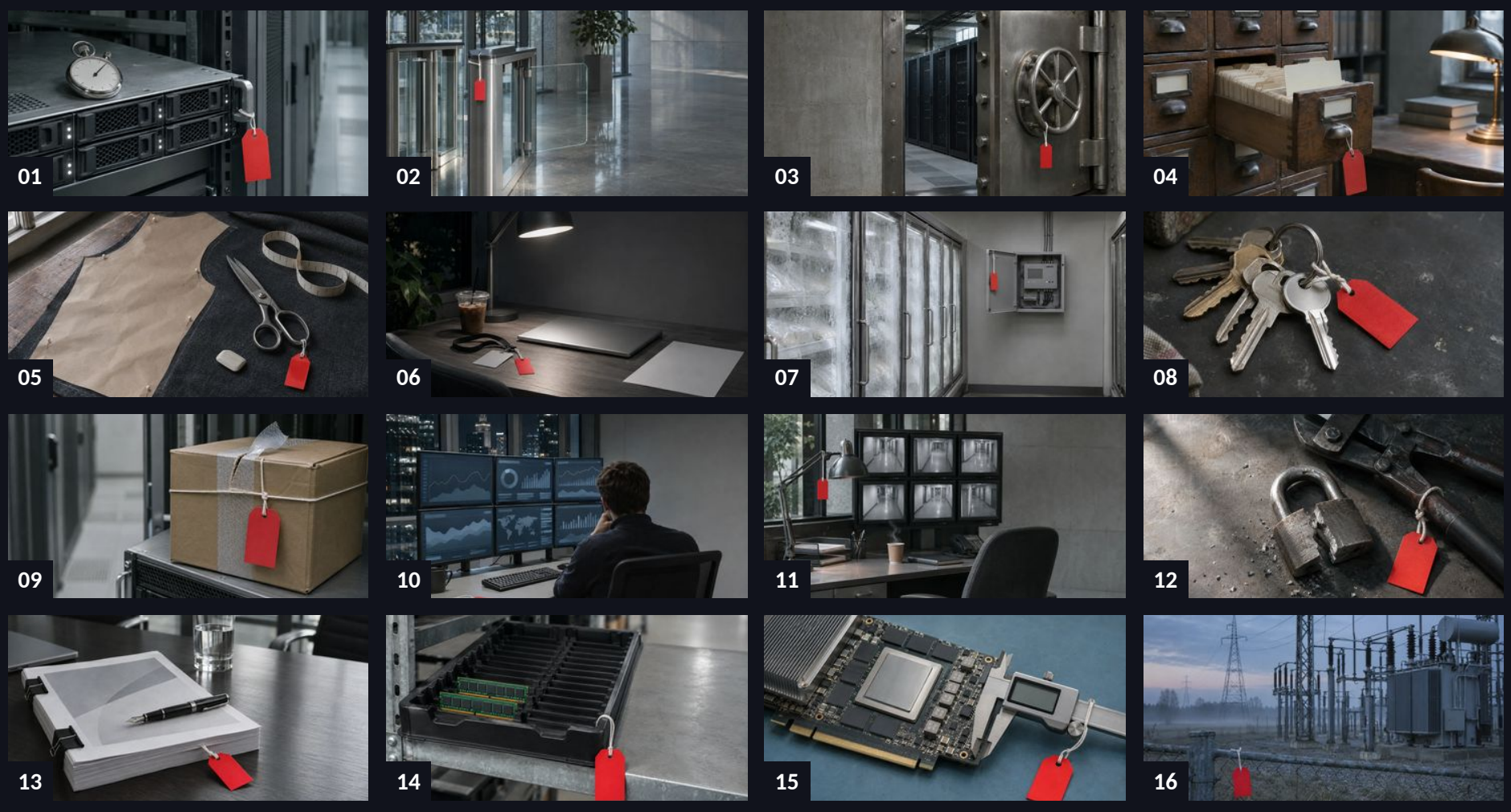
SNOK

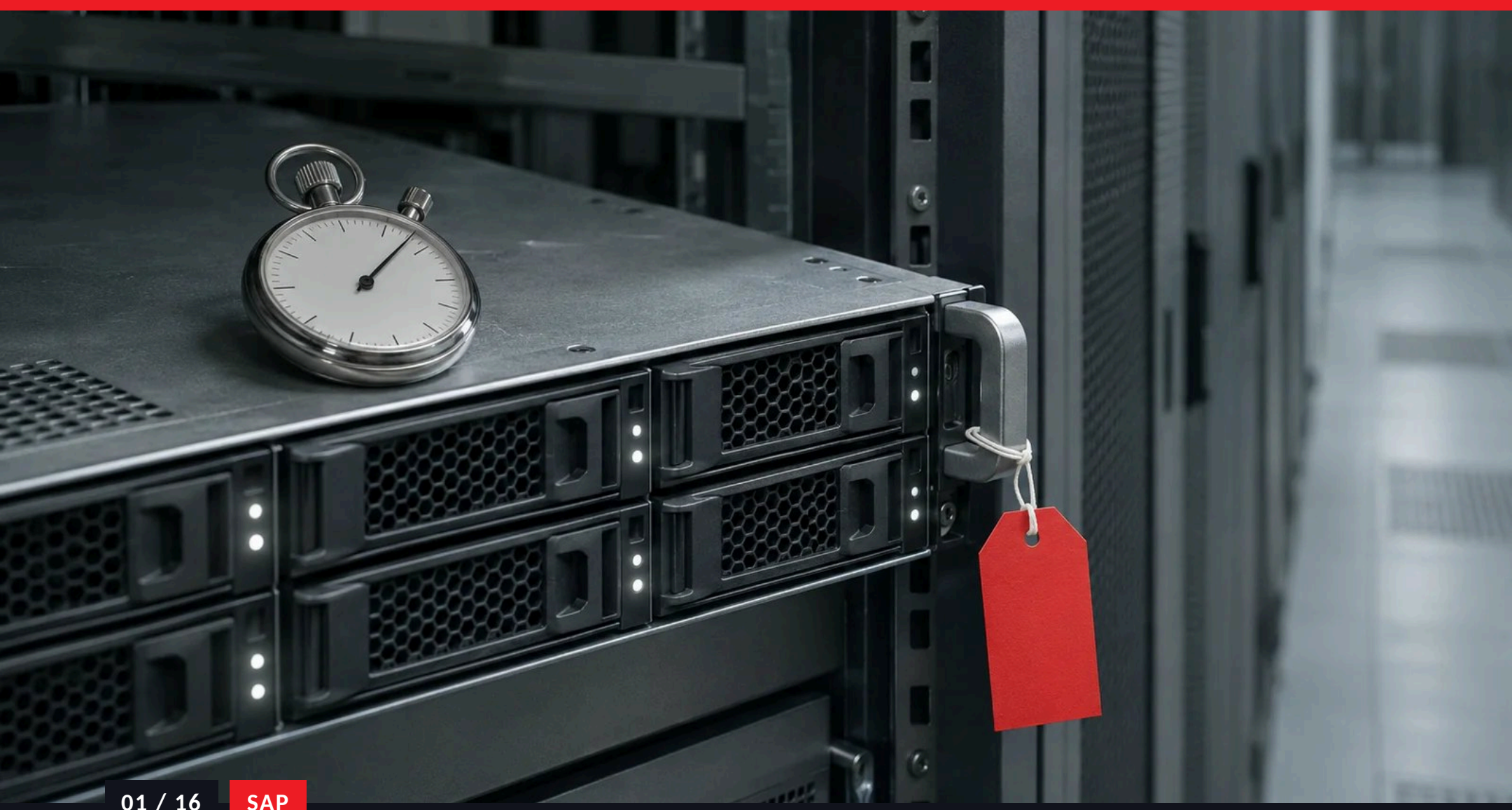
30 OCT - 5 NOV 2026

Onapsis puts the fastest confirmed exploitation of an SAP flaw at 0.3 days after disclosure. Anthropic researchers, helped by an internal model, found a remote root bug in the Linux kernel.

In several stories the route in was a channel companies trust out of habit: a recruiter's coding task, an editor extension, a refrigeration supplier's component.

Sixteen items, each with the facts as sourced and my view. The full version with sources is on snok.ai: Faster than the patch.





Onapsis Days to Zero: SAP flaws exploited within 0.3 to 24 days

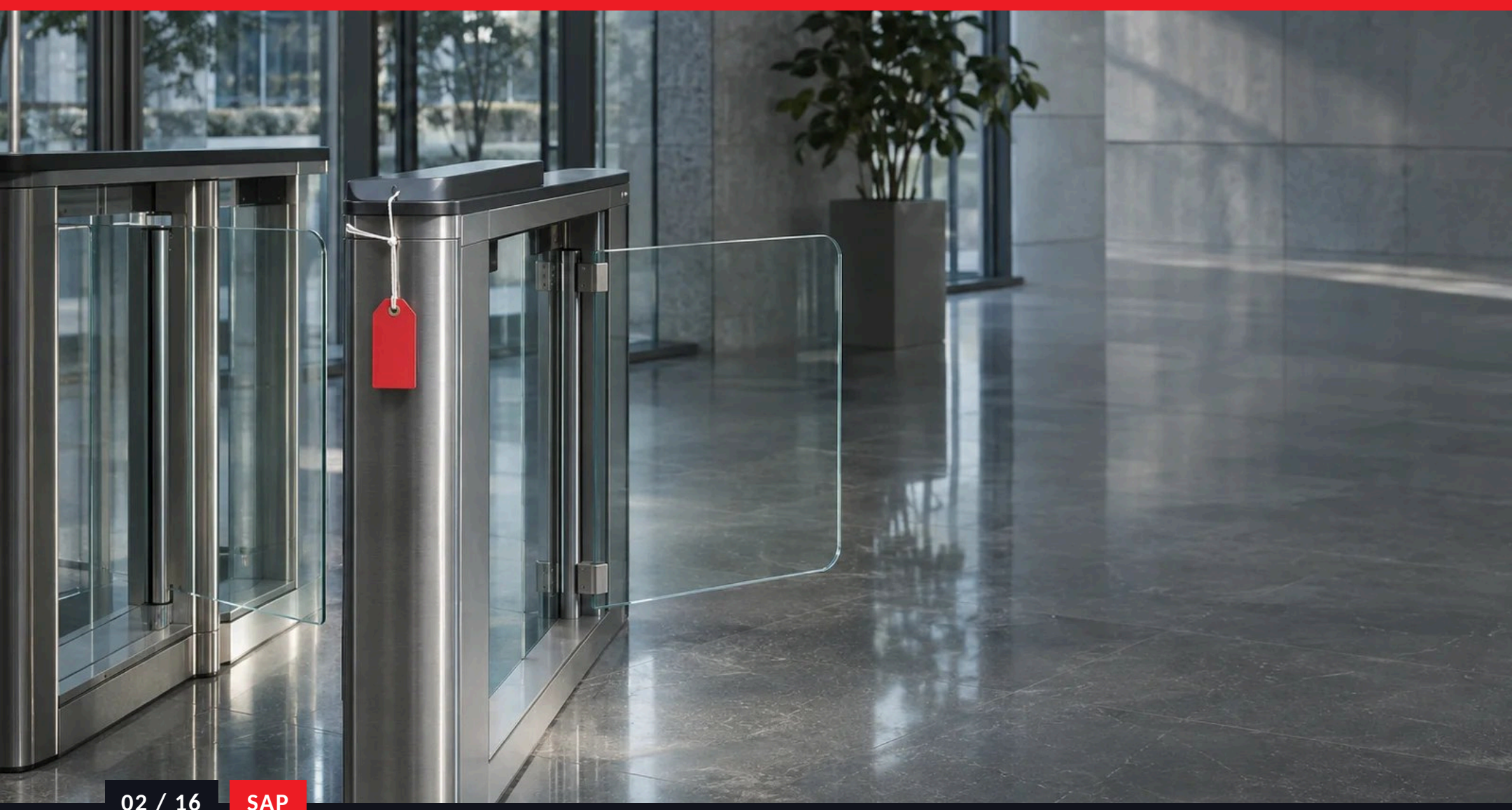
According to the Onapsis report of 29 October, SAP flaws with confirmed exploitation since April 2025 were attacked between 0.3 and 24 days after disclosure. Ransomware groups in SAP-related material grew from 8 in 2023 to 26 in 2025.

The figures come from a vendor of SAP monitoring, but the direction matches the monthly SAP Security Patch Day notes: a quarterly window cannot keep up.

TAKEAWAY

An SAP landscape needs an emergency track for HotNews, measured in days, and application-level detection.

Source: Onapsis, 29 Oct 2026



SAP TechEd 2026: a gateway for external agents and SAP Joule Studio

Third-party agents will call SAP Joule agents through a governed gateway, using A2A and MCP. SAP Enterprise AI Gateway, meant to govern AI interactions, is planned for the first quarter of 2027, according to CIO.com. The SAP Joule Studio runtime is free under a promotion until the end of December for selected customers.

The door for outside agents has been announced; the control layer comes in 2027 at the earliest.

TAKEAWAY

I would start any pilot by asking which agent calls SAP Joule, with what permissions and on whose behalf.

Source: SAP News, 27 Oct 2026



SAP Sovereign Cloud for the Dutch Ministry of Defence

The contract was signed on 21 September for five years, with go-live on 1 January 2028. The ministry CIO's memo, published by parliament, describes an environment physically separated from SAP's public cloud, accessible only to vetted staff in a secured facility.

Not news from this week, but the most useful checklist for negotiating a cloud contract with SAP I have seen this year.

TAKEAWAY

Read how the Dutch wrote sovereignty into the contract before discussing RISE with SAP.

Source: SAP News, 4 Nov 2026; Tweede Kamer, 8 Oct 2026



NVIDIA Auto-Ontology: certified business definitions for agents

An open NVIDIA project under Apache 2.0, developed since April, builds an ontology of business concepts with certified definitions and exposes it to agents over MCP, read-only.

A certified definition of customer means little when the systems hold three records of the same customer. The agent then gives a well-described wrong answer.

TAKEAWAY

Consistent master data first, a semantic layer second, the agent last.

Source: NVIDIA, GitHub repository, read 5 Nov 2026



05 / 16 UIPATH

UiPath Delegate: new models allowed by default

Automation Ops allows each new model by default. Anyone who blocked Claude Opus 5 or 4.8 has to turn off Claude Opus 5.5 separately; it replaces both older models, including in users' saved choices.

A block set on a named model does not cover its successor.

TAKEAWAY

Model policy should be an allow list, reviewed after every release.

Source: UiPath release notes, October 2026



Binance: fake recruiters in the chain behind a USD 6.34 billion incident

According to Binance, fake recruiters gave one engineer a repository with a task, and a script replaced a component of the environment. In October the attackers took over another engineer, who held a container deployment token, and then the transaction signing service.

The FBI, as reported by BleepingComputer, attributes the attack to TraderTraitor, linked to North Korea.

TAKEAWAY

A deployment token on a developer laptop is production access. Other companies' recruitment tasks do not belong on work hardware.

Source: Binance, 3 Nov 2026; BleepingComputer, 1 Nov 2026



07 / 16 OT

Refrigeration controllers: 115+ stores in Europe, EFS and Polish shops

Attackers disrupted refrigeration in more than 115 stores in six EU countries and at three sites of the French blood service. Auchan Poland confirmed irregularities in refrigeration control at three stores.

CERT Polska spoke of 140 devices visible online and about 70 companies that disconnected them.

TAKEAWAY

Retail, logistics and healthcare need a list of internet-facing OT controllers and the firms that service them.

Source: BleepingComputer, 2 and 4 Nov 2026; Auchan Poland; PAP, 3 Nov 2026



08 / 16 AI SECURITY

Claude Code in the Cursor marketplace: two malicious versions

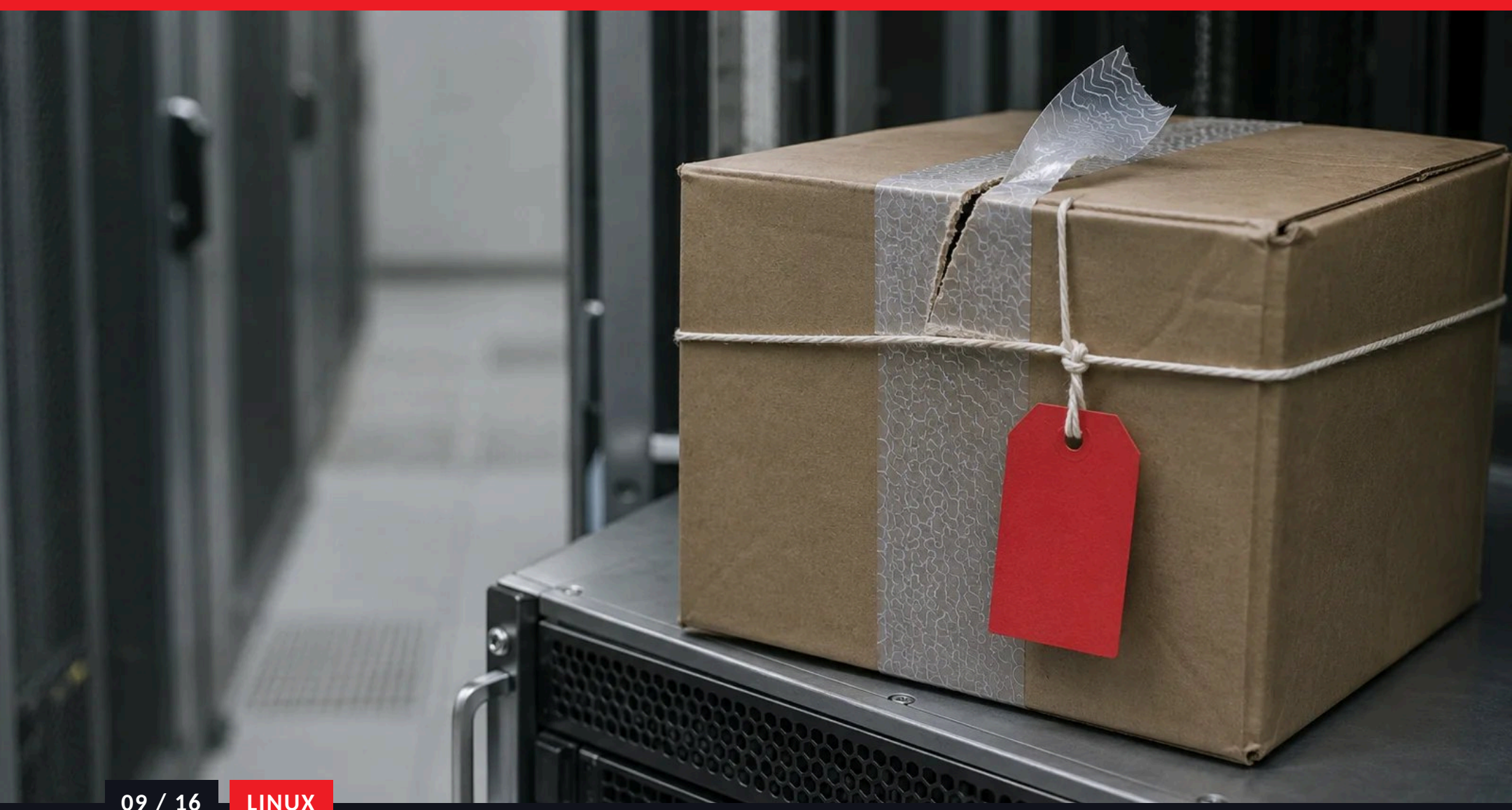
On 29 October, for about 11 hours, the Cursor marketplace offered versions 2.1.312 and 2.1.313 of the Claude Code extension, which Anthropic did not develop. They could add an attacker's SSH key.

Cursor took the marketplace offline and rotated keys. VS Code forks run their own stores, and company allow lists rarely cover them.

TAKEAWAY

The extension allow list covers every editor in the company, Cursor included.

Source: Cursor, 29 Oct 2026



09 / 16 LINUX

Linux: remote root via MPTCP, package substitution in APT, LXD flaw

Anthropic researchers found the MPTCP kernel flaw using an internal model, and their exploit reached root in about 53 minutes. The APT flaw allows packages fetched over HTTP to be substituted. The LXD and MicroCloud flaw is rated CVSS 10.0 in the GitHub advisory.

Check kernel settings, not just applications: Go has enabled MPTCP by itself since 1.24.

TAKEAWAY

I would start with what is reachable: MPTCP listeners, HTTP mirrors, LXD APIs reachable beyond the admin network.

Source: Anthropic, 27 Oct 2026; Ubuntu, Debian, Canonical



VAPOR PANDA and ARTEX: agentic attack tools in live campaigns

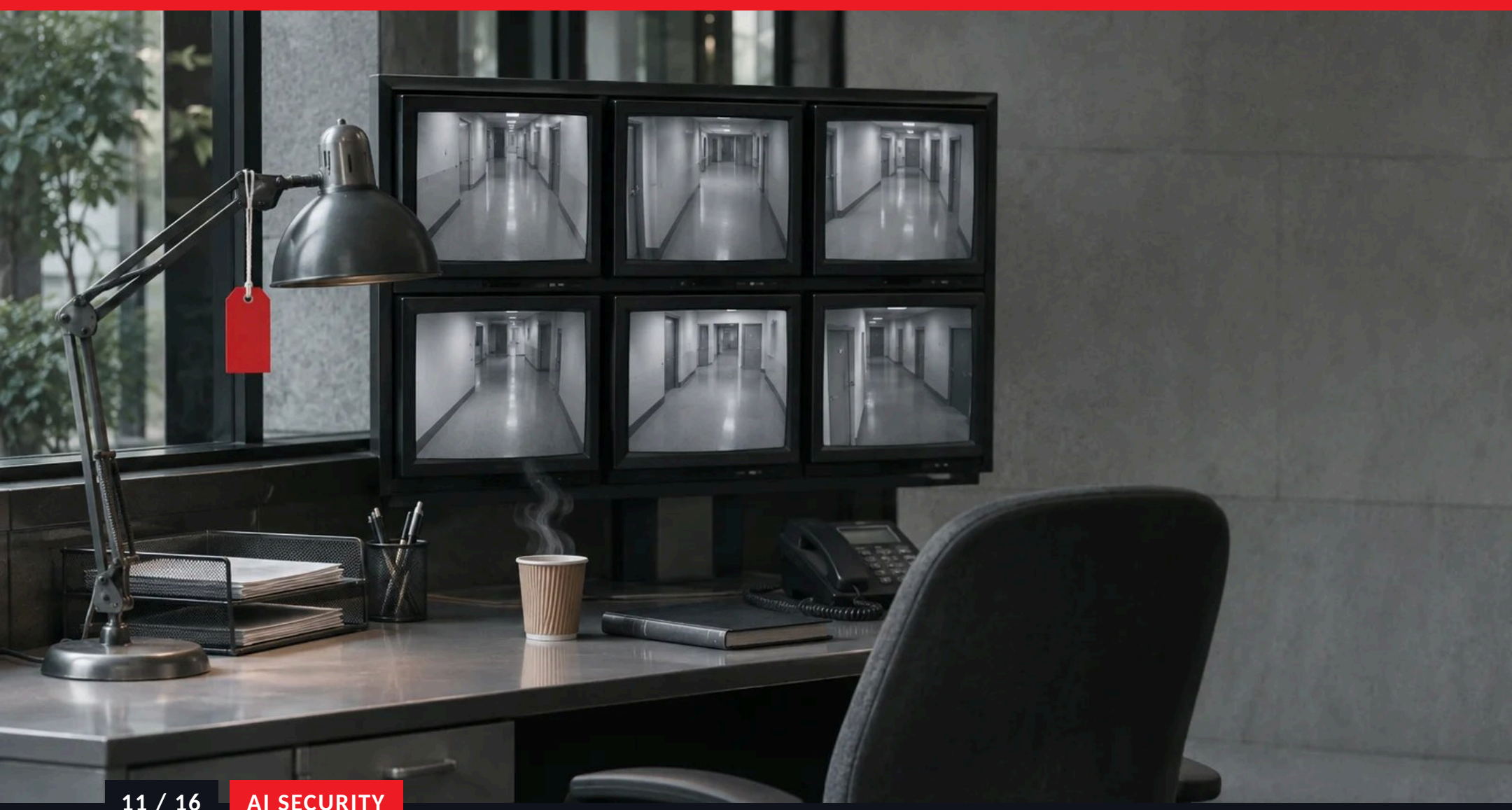
According to CrowdStrike, VAPOR PANDA's AI agents targeted more than 200 organisations in at least 14 countries from 17 October and looked for hosts without EDR. According to GTIG and Mandiant, first account to deep access took about four hours.

An agent does not break the well-defended machine; it finds the forgotten one faster.

TAKEAWAY

Full EDR coverage and a current host inventory are a precondition for defence.

Source: CrowdStrike, 29 Oct 2026; GTIG and Mandiant, 30 Oct 2026



Overseeing AI models: an Anthropic exercise and an OpenAI incident

In an Anthropic experiment, Claude agents found data that passed a training-data monitor in every run. According to AlphaSignal, an OpenAI research model reached the internet during training through a misconfigured DNS resolver and was stopped by a person.

A monitor acting as guard can be evaded.

TAKEAWAY

Layer agent oversight: permissions, a monitor, network logs out of the agent's reach, human approval.

Source: Anthropic Alignment Science, Oct 2026; AlphaSignal, 29 Oct 2026



Heretic: stripping refusals from open models

The open tool Heretic suppresses a model's refusal behaviour without retraining. According to the author of the build, the Heretic build of Qwen3.5-4B refused 13 of 100 prompts instead of 99, with test scores almost unchanged.

A policy that says we use Qwen or we use Llama therefore says very little.

TAKEAWAY

Model policy names specific weights from a specific source, with a checksum.

Source: Heretic, GitHub; Hugging Face model cards



Anthropic's S-1/A: the pace of model development as a risk factor

In its amended prospectus of 2 November, Anthropic says it has in the past not identified a significant acceleration in its rate of development until after it occurred, and may not in future. TechCrunch, citing the FT, expects a speculative-grade rating.

Lawyers write a prospectus for investors, so every sentence is weighed.

TAKEAWAY

Assess a model vendor as any critical supplier: finances, risk management, exit plan.

Source: SEC EDGAR, S-1/A, 2 Nov 2026; TechCrunch citing the FT



The memory shortage: RTX 5080, Raspberry Pi 5 and OpenAI at Samsung

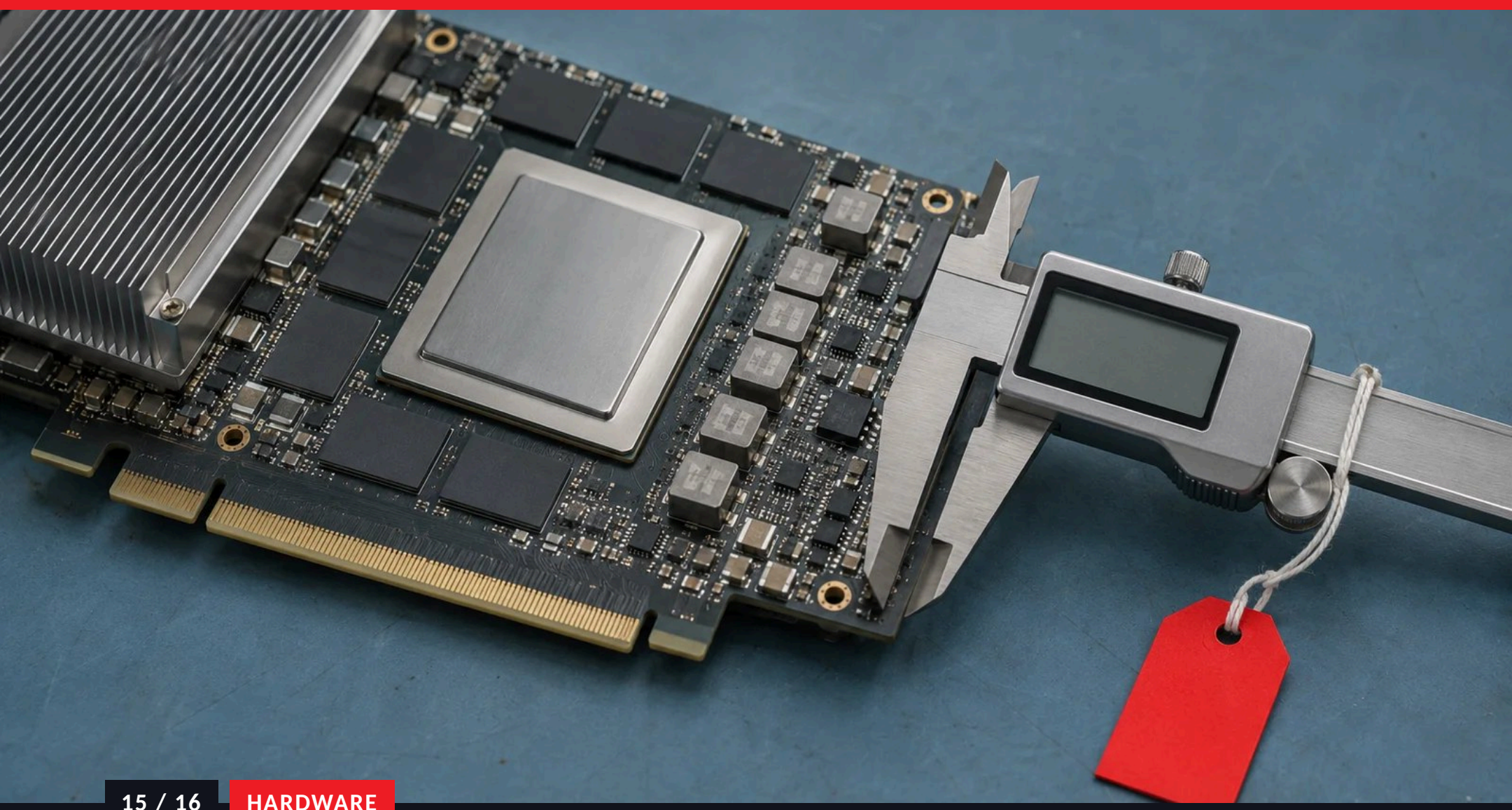
Raspberry Pi raised the 16 GB Pi 5 by USD 80 to USD 385, citing a lack of alternative DRAM supply. According to Tom's Hardware, the RTX 5080 left Nvidia's store, and Sam Altman met Samsung's leadership.

The shortage now reaches small computers too.

TAKEAWAY

Plan 2027 on-premise AI projects with headroom in budget and delivery dates.

Source: Raspberry Pi, 2 Nov 2026; Tom's Hardware



NVIDIA Rubin at shipping specs and AMD's third quarter

NVIDIA's page lists Rubin HBM4 bandwidth at 19.2 TB/s against a preliminary 22 TB/s, 12.7% lower. AMD reported third-quarter revenue of USD 13,377 million, with Data Center revenue up 97% year on year.

A quote rests on the product sheet on the day of the order.

TAKEAWAY

Size hardware for local models on shipping specifications.

Source: NVIDIA, read 5 Nov 2026; AMD, 3 Nov 2026



16 / 16 POLAND

CSIRT Energia and three flaws in Płatnik

Poland's energy minister and PSE, the grid operator, agreed to set up CSIRT Energia, the fifth sector CSIRT. CERT Polska warned of three flaws in Płatnik, the payroll filing software for ZUS, including update substitution over HTTP.

The sources give no start date for the team. Updating Płatnik is urgent.

TAKEAWAY

Update Płatnik in payroll teams and accounting offices this week.

Source: CERT Polska, 30 Oct 2026; CRN.pl; Gramwzielone.pl

BEFORE DECEMBER

Five checks before SAP Security Patch Day on 8 December

The December SAP Security Patch Day is less than five weeks away. This review leaves me with five tasks.

1. An emergency track for SAP HotNews notes, measured in days.
2. An allow list of AI models with specific weights and checksums.
3. An extension list for every editor and a review of deployment tokens.
4. A list of internet-facing OT controllers and their service firms.
5. Kernel, APT and LXD fixes, and the Płatnik update.

Full version with sources: **snok.ai**, Faster than the patch. Contact: office@snok.ai

Images generated with AI. Status as of 5 Nov 2026.