

SNOK

WEEKLY REVIEW W46

Key under the doormat

SNOK's review of 6-12 November 2026: SAP Security Patch Day, agents in UiPath and airline booking, OpenSSH and Outlook, device code phishing, secrets in agents' files, new models from OpenAI and Anthropic, and Nvidia's CEO resignation

Swipe →

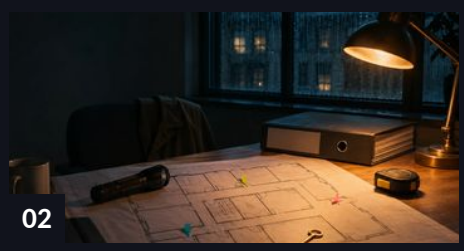
6-12 NOV 2026

Four SAP notes carry a CVSS score of 10.0 and concern components that handle network traffic. An OpenSSH flaw opens, in certain configurations, to a very long password. A coding agent sometimes saves passwords in a settings file that users add to public repositories.

In several of this week's stories, access was left where anyone could look.

Thirteen topics follow, each with the facts as the sources state them and my comment. The full version with sources is on snok.ai.

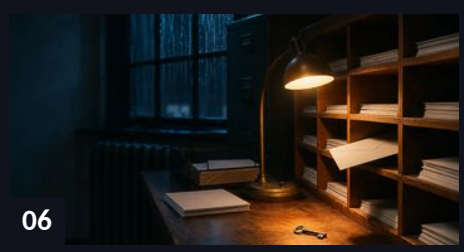

01


02


03

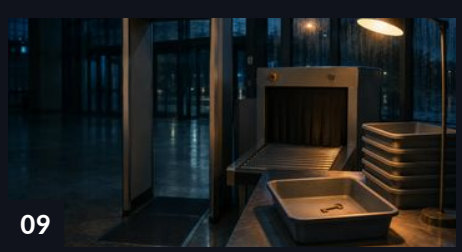

04

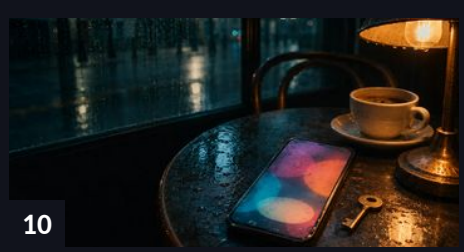

05

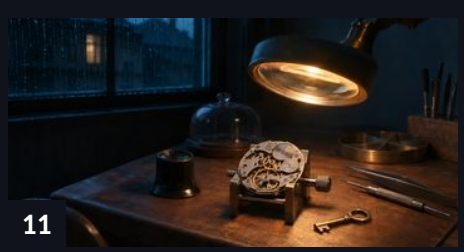

06

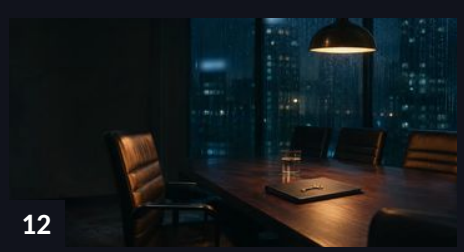

07

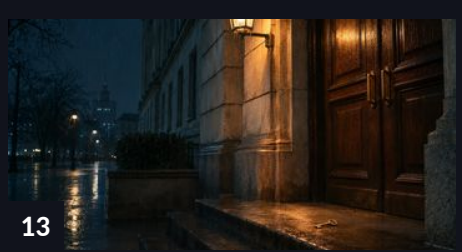

08


09


10


11


12


13



01 / 13 SAP

SAP Security Patch Day: 42 items and four notes rated 10.0

On 10 November SAP published 42 items, nine of them critical. Four notes carry a CVSS score of 10.0: ICM in AS ABAP, SAP Web Dispatcher, SAP Gateway and the SAML2 service in AS ABAP.

A maximum score means a network attack with no privileges and no user interaction. All four sit in the entry layer: HTTP, RFC and federated sign-in. SAP does not say whether the flaws are exploited. The next Patch Day is on 8 December.

TAKEAWAY

This month, plan a kernel update and check which ICM, Web Dispatcher and Gateway instances are reachable from outside the internal network.

Source: SAP Security Notes, 10 Nov 2026



The OWASP SAP Pentest Playbook: an open catalogue of SAP testing techniques

The OWASP Core Business Application Security project maintains a public catalogue of SAP penetration testing techniques under CC BY 4.0. SecuritySilverbacks has maintained the repository since May 2025; the latest change is from 7 November. Its sponsors include SecurityBridge, with which we are partners.

It is a community effort at Incubator stage, with no standing as an OWASP standard, but a useful shared vocabulary for the board, the Basis team and the tester.

TAKEAWAY

Before the next SAP pentest, ask the supplier which techniques on this list it covers and which it leaves out.

Source: GitHub, SecuritySilverbacks; OWASP



UiPath as a launch partner for Gemini for healthcare

Through the UiPath MCP Server, Gemini can start an automation, check its progress or hand a task to a UiPath agent, with the platform's existing access controls and audit. The integration is in preview for joint UiPath and Google Cloud customers.

The model holds the conversation; execution runs through a platform with permissions and audit. Availability in the EU has not been confirmed.

TAKEAWAY

The pattern of a model calling a governed automation through MCP is worth assessing on your own process now.

Source: UiPath, 10 Nov 2026



United will not let third-party AI agents complete bookings

According to The Verge, citing the Wall Street Journal, United Airlines will not let third-party AI assistants complete a booking on a user's behalf. Agents can still search for and show flights.

The airline cites data protection, unintended purchases and disclosure rules in ticket sales. The airline has left room to revisit the decision.

TAKEAWAY

Connecting an agent to someone else's system should go through an agreed, authenticated integration.

Source: The Verge, 11 Nov 2026



SSHole: bypassing OpenSSH password login on musl

CVE-2026-123158 affects sshd on Linux with musl and no PAM, with password login enabled. For some accounts with an asterisk in the password field, any password over 256 bytes and up to 1,024 works, provided another account has a valid hash. Alpine ships this way by default.

OpenSSH 10.6p2 works around it. CISA added the flaw to its exploited vulnerabilities catalogue on 9 November. Dropbear and glibc or PAM systems are not affected.

TAKEAWAY

Inventory images and devices on musl; until updated, set PasswordAuthentication no once key login is confirmed.

Source: OpenSSH; CISA KEV



Microsoft Patch Tuesday: one exploited flaw, in Outlook

According to Tenable, Microsoft fixed 1,093 flaws in its own products, or 1,235 with 142 in Edge. The only one marked as exploited is CVE-2026-124194 in Outlook: opening a crafted message file leaks the NTLMv2 hash. Rated Moderate, CVSS 6.5, with a CISA deadline of 24 November.

The fix ships through Microsoft 365 Apps, not the Windows cumulative update.

TAKEAWAY

A team that patches only servers and the OS will miss it. SAP notes and Microsoft fixes are two separate channels this week.

Source: Tenable; BleepingComputer; CISA KEV



Device code phishing dressed up as AI events

Push Security described fake event invitations using the OpenAI and SpaceX brands, with prizes such as three months of ChatGPT Pro. The victim types a code into Microsoft's real page and authorises the attacker's device themselves.

A stolen Entra token opens apps connected through single sign-on, including Microsoft 365, Salesforce, Atlassian and SAP.

TAKEAWAY

A correct address bar offers no protection. Never enter a code you did not request; in Entra, restrict device code.

Source: Push Security; BleepingComputer, 5 Nov 2026



08 / 13 AI SECURITY

Claude Code: passwords in the "don't ask again" file

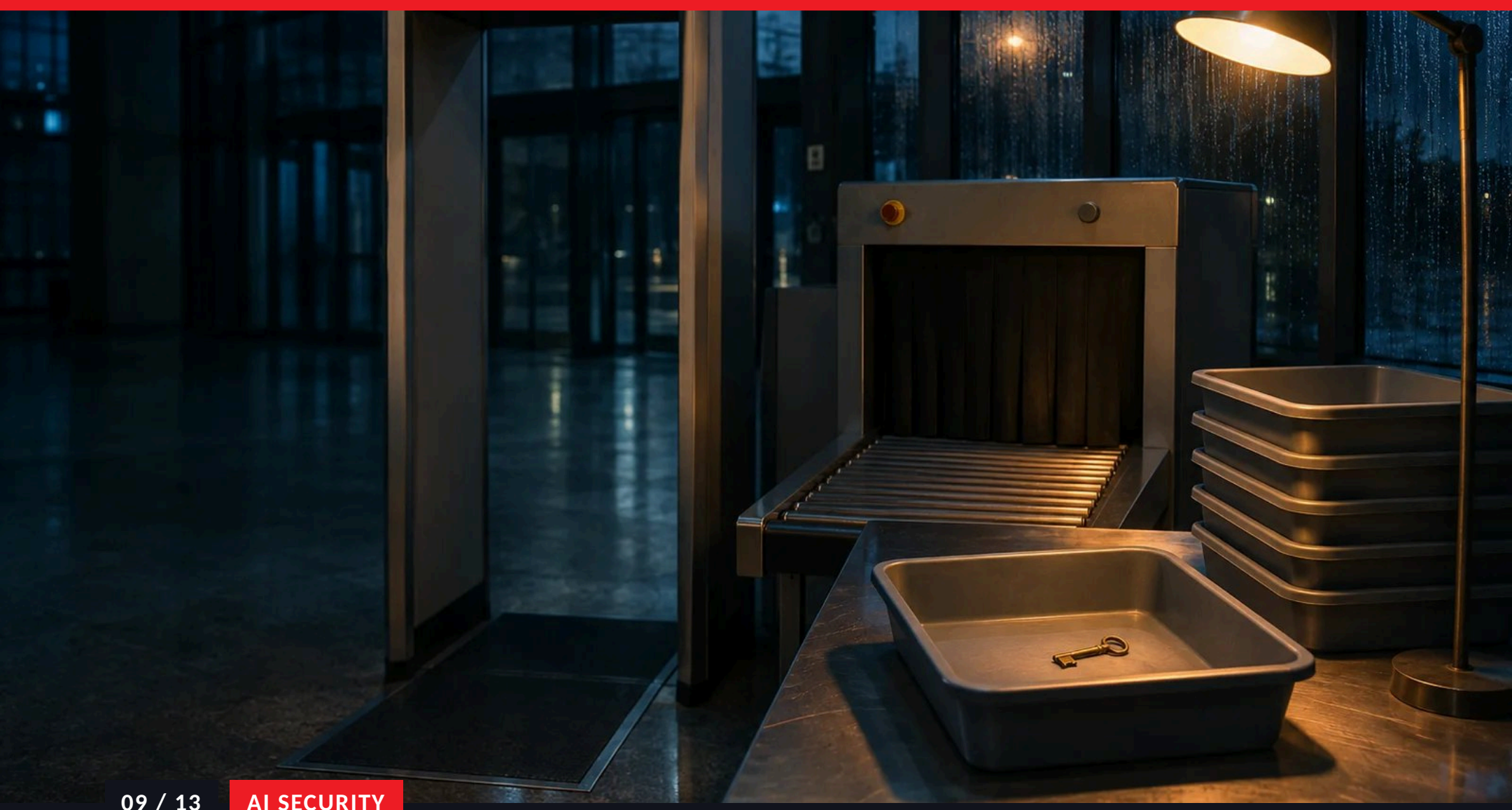
According to The Hacker News, Apiiro found secrets in 1,122 of 104,185 copies of .claude/settings.local.json in public repositories, 1,379 distinct secrets: database passwords, SSH credentials, tokens and AWS keys. Neither gitleaks nor TruffleHog flagged them in 215 files.

The file stores commands approved with "don't ask again", sometimes with a password in them. Users add it to repositories; Claude Code does not put it in the project's .gitignore.

TAKEAWAY

Treat coding agents' directories like .env files: add them to .gitignore, scan history and rotate passwords.

Source: The Hacker News, reporting Apiiro, 7 Nov 2026



OpenAI GPT-6 Cyber for a small circle of researchers

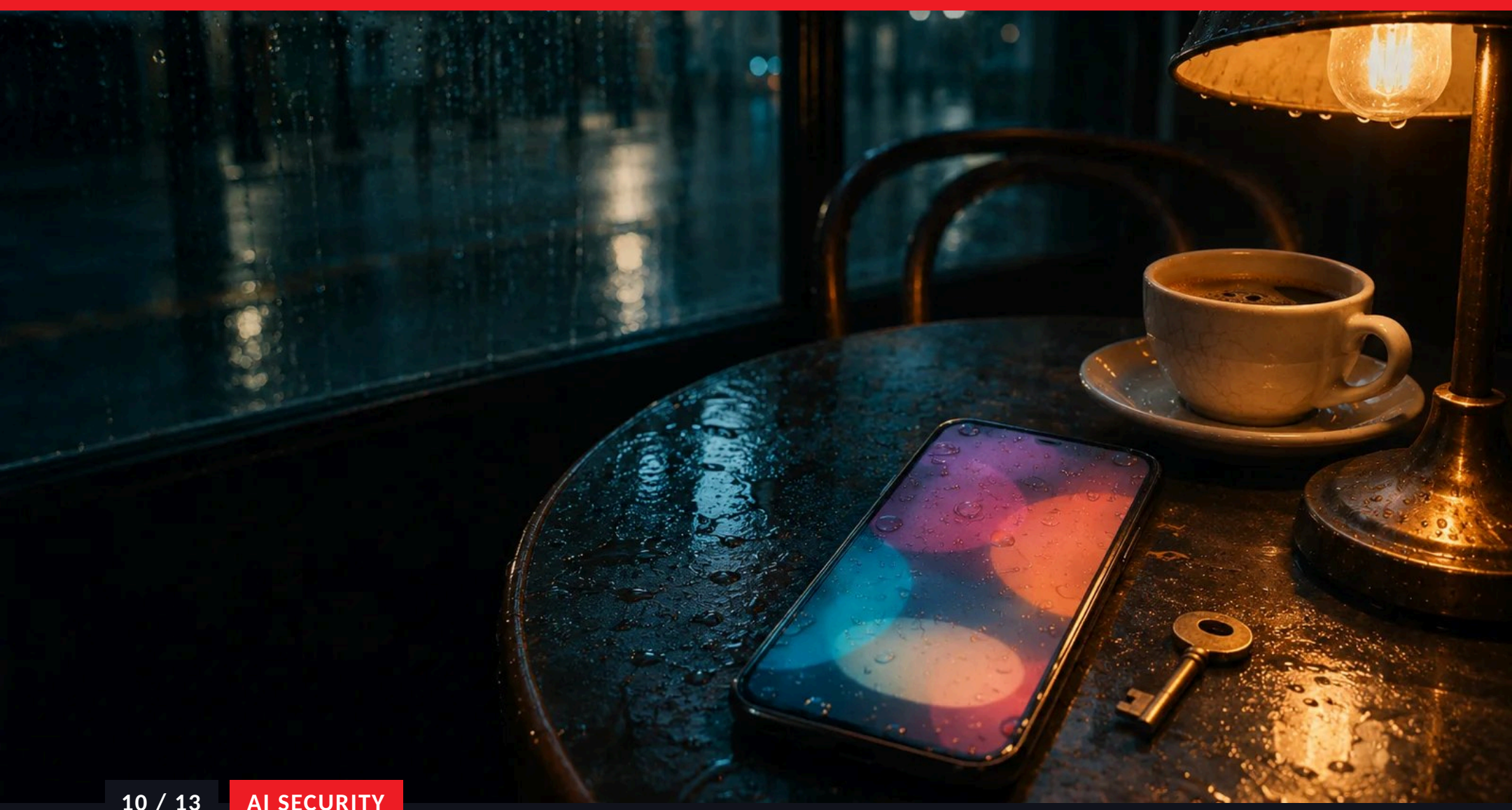
OpenAI announced GPT-6 Cyber for selected Daybreak Red customers. OpenAI says it produced exploits for 948 Linux kernel vulnerabilities and found 81 unknown flaws in Firefox. Mozilla's MFSA 2026-118 credits OpenAI with 41 entries; 81 may span other advisories.

The figures are the vendor's. Mozilla's advisories and OpenSSH's release notes already credit AI-assisted reports.

TAKEAWAY

If reports keep growing, I would make room in next year's budget for a shorter patch cycle.

Source: BleepingComputer; TechCrunch; Mozilla



A mobile agent sees something different from a person

The arXiv preprint "When Agents See Differently": 546 tasks, 13 apps, 5 agent frameworks and 3 models.

The average rate at which the agent was misled, picking the control chosen by the attacker, was 77.4 per cent in static evaluation and 67.2 per cent in dynamic evaluation, at app level.

TAKEAWAY

Screen-based automation needs human confirmation before irreversible actions.

Source: arXiv 2609.16732 (preprint)



Claude Fable 5.2 and Mythos 5.2: 20 per cent less per token

One base model with different safeguards: Fable for everyone, Mythos for verified organisations. Compared with 5.1, the price fell from USD 10 to USD 8 per million input tokens and from USD 50 to USD 40 for output.

Both models voice suspicion that they are being evaluated more often than any recent Anthropic model. They require 30-day data retention; zero data retention only with Anthropic's approval.

TAKEAWAY

Before switching, customers under NIS2 or DORA should check retention and test agents in near-production conditions.

Source: Anthropic, 9 Nov 2026



Nvidia: Jensen Huang steps down

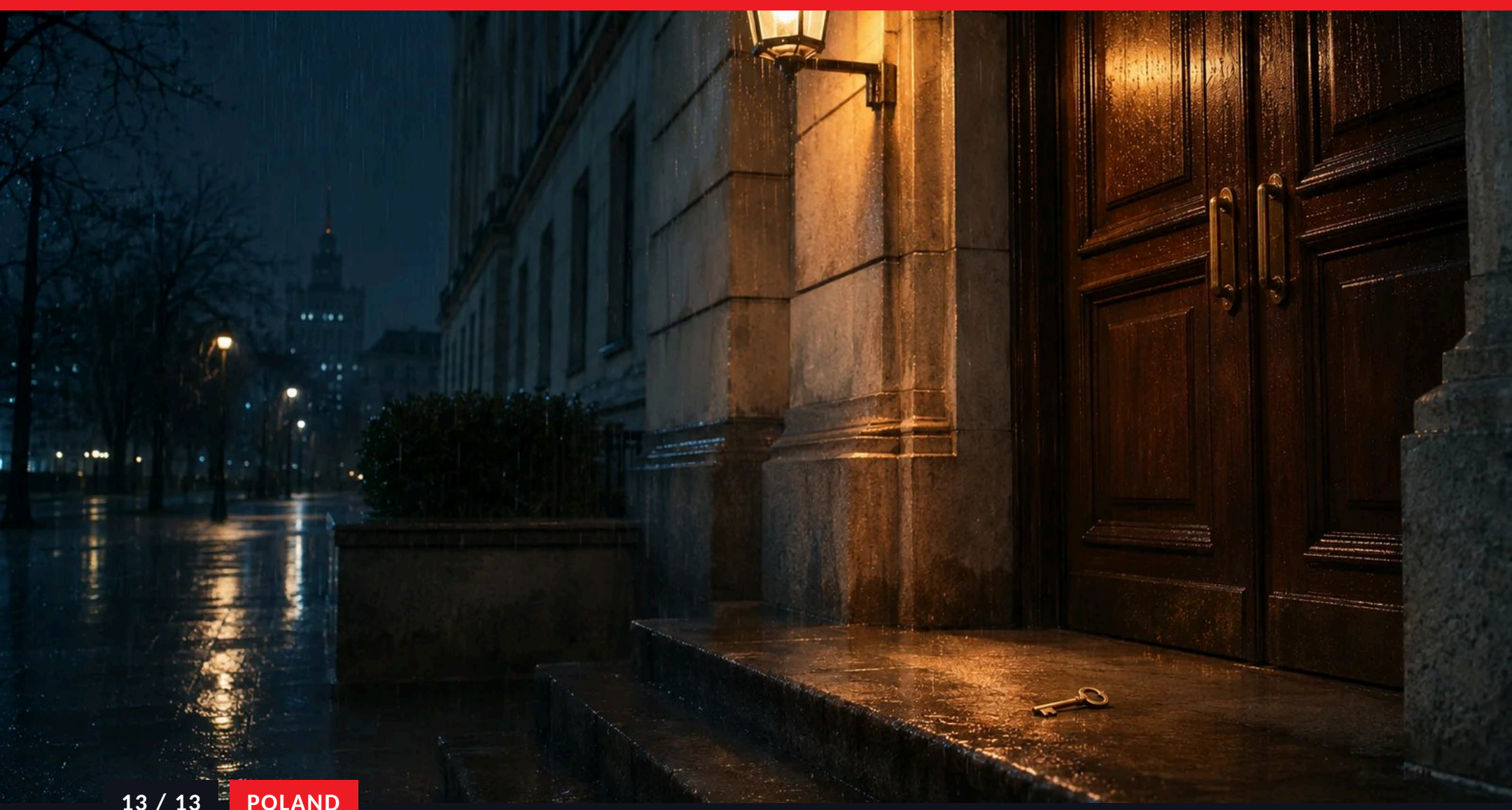
On 11 November the board accepted Jensen Huang's resignation with immediate effect. Colette Kress is acting CEO and Harvey C. Jones has become chair. The SEC filing gives no reason.

The resignation followed two weeks of media reports about the chief executive; the company does not link them. Q3 fiscal 2027 results: 17 November.

TAKEAWAY

With Nvidia under interim leadership, keep a fallback option for AI infrastructure purchases planned for 2027.

Source: Nvidia, Form 8-K, 11 Nov 2026



POLAND

Poland's digital ministry and Microsoft agree on cyber resilience

According to CRN.pl and the Polish Press Agency, the cooperation covers threat information sharing, protection of legacy systems, fast service restoration and AI for defence teams in public administration and critical infrastructure.

We found no ministry announcement. The media reports suggest no new legal obligations for companies.

TAKEAWAY

The administration's priorities are legacy systems and service continuity. Assessing KSC and NIS2 impact needs the ministry's announcement.

Source: CRN.pl; PAP, 10 Nov 2026

BEFORE 8 DECEMBER

Five checks before 8 December

Fewer than four weeks remain before December's SAP Security Patch Day. Here are five places where access may have been left under the doormat.

1. Which ICM, SAP Web Dispatcher and SAP Gateway instances are reachable from outside the internal network.
2. Which container images and devices run OpenSSH on musl with password login.
3. Whether the Outlook fix from the Microsoft 365 Apps channel has been checked separately.
4. Who actually needs the device code flow in Microsoft Entra.
5. Whether .claude, .cursor and .gemini are in .gitignore and whether repository history has been scanned.

Full version with sources: **snok.ai**, Key under the doormat. Contact: office@snok.ai

Images generated with AI. Status as of 12 Nov 2026.