THE 808

AI, CLOUD AND SECURITY FOR PEOPLE WHO SIGN THE CONTRACTS // FROM THE 808

NO. 11
NOVEMBER 2026
THE 808 BRIEF
FREE MONTHLY MAILER



> ./808_brief --edition=november

> WHO HOLDS THE KEYS?

$1.6B
Ottawa's stake in Cohere

9.2/10
CVSS score on PHP2Shell

Sovereign AI: what a $1.6B stake buys you
PHP2Shell: the patch your host owes you
LiteLLM, poisoned twice: lock your AI keys
Eight things that broke in October

THE COVER IS A CARTOON. EVERYTHING INSIDE IS CHECKED AGAINST A SOURCE YOU CAN OPEN YOURSELF.

LIVE // ◆ Bank of Canada hikes for the first time since 2023 ◆ Federal budget lands November 5 ◆ C

HI, BUILDERS.

Welcome to the November Brief. Once a month we take everything The 808 tracked across AI, cloud and security, and boil it down to the three stories that should change what you do next week.

October had a theme, and it's on the cover: keys. Ottawa bought a stake in a Canadian AI company so Canadians hold more of their own keys. Meanwhile, attackers went after the software that holds everyone else's: PHP itself, and the AI gateways that store your model API keys.

New this month: every feature ends with a CONNECTED box. It links to related stories in this issue and in our four sister mailers. Our sports mailer, for one, read the Cohere deal next to Saudi Arabia's football money. Every number still carries a superscript that points to a source at the back. Spot a mistake? contact@the808.org.

THE 808 // THE 808

THIS ISSUE IN NUMBERS

$1.6B
maximum federal equity stake, paid in stages

1,000+
new technical jobs Cohere must create by 2030

$1.7B
new Canadian compute Cohere commits by 2030

$700M
Regional AI Initiative total after Oct 13

From the PMO release and FedDev Ontario.[1,2]

CONTENTS

The comic: The Key Heist 3

Feature: Ottawa buys a seat at the AI table 4

Feature: PHP2Shell is the patch your web host owes you this week 1

Feature: Your AI plumbing is now an attack surface 10

The crawl: this month's other stories 13

The wire: how our mailers connect 15

Sources: check our work 16

HOW TO READ THIS ISSUE

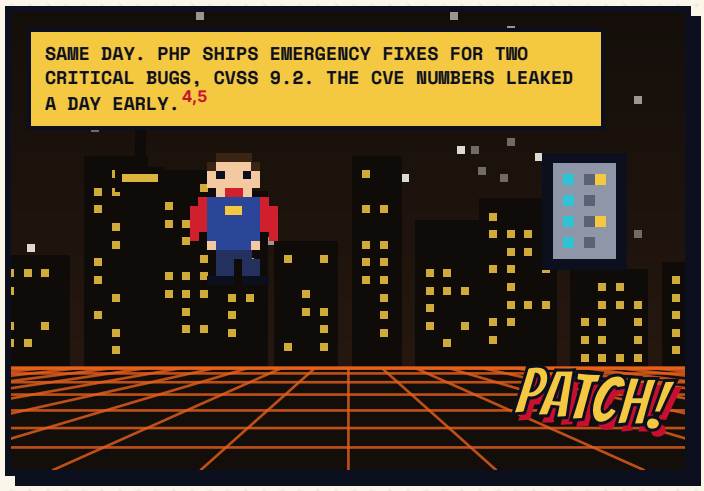
- ☑ A blue check means a fix is available today.
- ☐ An empty box means there is no fix yet.
- ⍰ A question mark means we couldn't confirm it either way.

Risk ratings are our call. The facts under them are not.

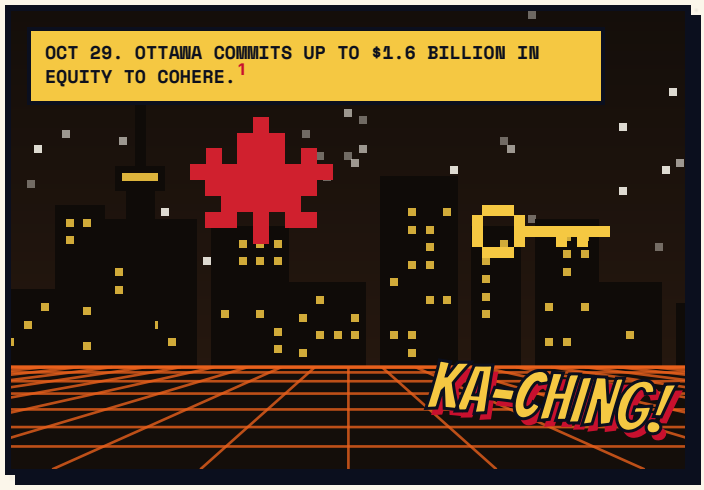
THE 808 COMICS PRESENTS

THE KEY HEIST! CHAPTER 10









THE SCORECARD

☑	**PHP 8.2–8.5**	Patched Oct 21
☐	**PHP 8.1 and older**	End of life, no fix
☐	**CVE-2026-115560**	Mitigation only
☑	**LiteLLM 1.107.0**	Pulled; rotate keys
?	**AI Gateways category**	No scored products yet

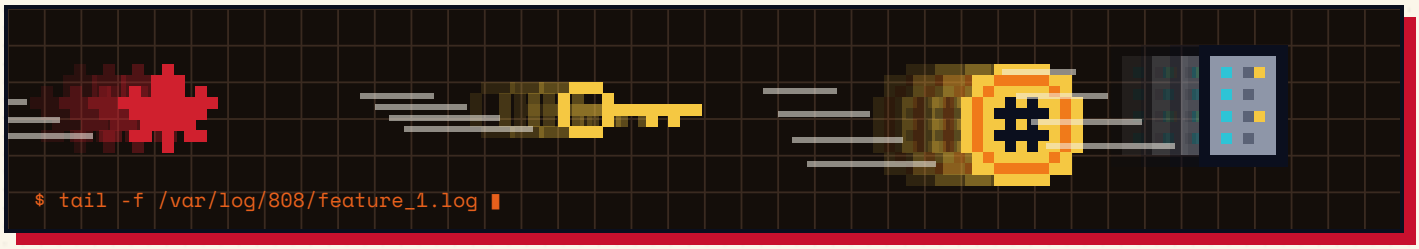
Checks, boxes and question marks are explained on page 2. The comic is a cartoon; every caption is sourced.

TO BE CONTINUED...

The comic is the pitch. Turn the page for the reporting, the numbers behind every panel, and our take.

$ OTTAWA BUYS A SEAT AT THE AI TABLE

What a $1.6 billion federal stake in Cohere actually changes for Canadian IT buyers



$1.6B
maximum federal equity stake, paid in stages

1,000+
new technical jobs Cohere must create by 2030

$1.7B
new Canadian compute Cohere commits by 2030

$700M
Regional AI Initiative total after Oct 13

From the PMO release and FedDev Ontario.[1,2]

For two years the phrase "sovereign AI" has mostly lived in slide decks. On Thursday, October 29, it got a price tag. Prime Minister Mark Carney stood up in Montréal and announced that the Government of Canada will make an equity investment of up to $1.6 billion in Cohere,[1,7] the Toronto-founded company that builds large language models and enterprise AI systems for businesses and governments.

This is not a grant. Ottawa is framing it as a commercial investment, made alongside private money from NVIDIA, Bell and Germany's Schwarz Group, and paid out in stages. In return, the government gets an ownership stake and a set of conditions that read like a sovereignty checklist.[1]

WHAT COHERE SIGNED UP FOR

According to the Prime Minister's Office, Cohere has committed to:

- Create at least 1,000 new high-paying technical jobs in Canada by 2030.
- Spend at least $1.7 billion on additional computing infrastructure in Canada by 2030.
- Keep its Canadian incorporation and Canadian headquarters.
- Invest in Canadian research partnerships and student opportunities.
- Keep working with the Canadian AI Safety Institute.[1]

Cohere also has to report regularly on progress against those jobs and investment commitments, and the money is released in tranches. The release also notes that Cohere recently merged with Germany's Aleph Alpha, which gives the company a European foothold to go with its Canadian one.[1]

WHY NOW

The Cohere deal is the biggest move yet in a busy month for federal AI policy. On October 2, Carney launched a new National Council on Artificial Intelligence under the *AI for All* strategy that Ottawa first announced in June.[8] On October 13, AI Minister Evan Solomon opened another $500 million over five years for the Regional Artificial Intelligence Initiative, bringing that program to $700 million in

total.[2] That money flows through the regional development agencies to help ordinary businesses adopt AI, not just build it.

Put those together and the shape of the policy becomes clear: fund adoption at the bottom, back a national champion at the top, and tie both to the idea that Canadians should have a credible, Canadian-controlled option.

THE PART THE PRESS RELEASE DOESN'T ANSWER

Here's what I'd want any CIO to sit with before rewriting their AI roadmap.

First, the release doesn't say whether federal departments will actually *use* Cohere. It says the investment gives Canadian businesses and governments more choice. Choice is good. It isn't a procurement commitment, and it isn't a guarantee of lower prices or better models.

Second, sovereignty is more than geography. A model hosted in a Canadian data centre is a start, but buyers should also ask who holds the encryption keys, which country's laws can compel access to the data, where support staff sit, and where model updates are trained. Those questions apply just as much to the big U.S. hyperscalers as they do to Cohere.

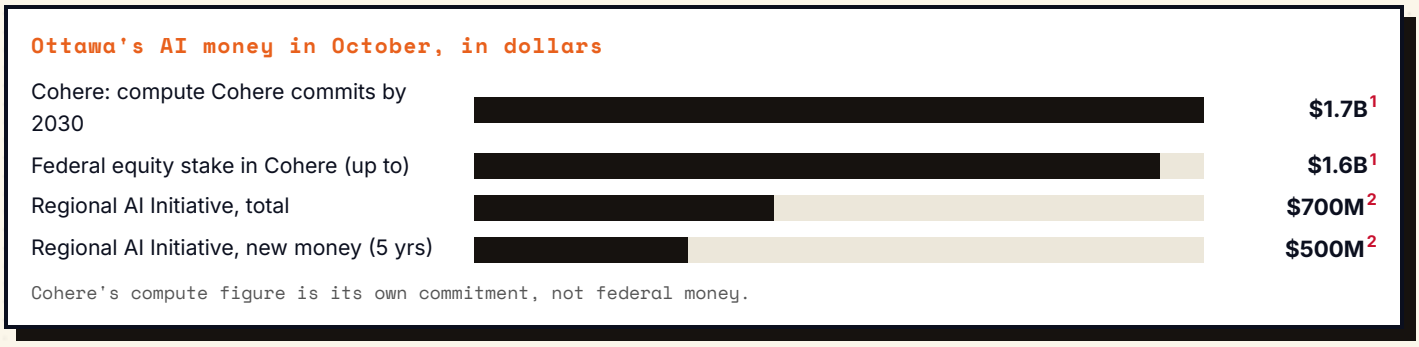
Third, there's a real debate about whether national control translates into public accountability. An October 26 essay in *Open Canada* argued that a Canadian-controlled AI system can reduce dependence on foreign infrastructure without making automated decisions any easier for citizens to understand or contest.[9] On the other side of the aisle, Conservative MP Leslyn Lewis wrote in *The Hill Times* on October 28 that Canada needs its own capacity rather than relying on systems shaped in the U.S. or China.[10] Both arguments can be true at once, and both are worth reading.

WHAT THIS MEANS IF YOU BUY AI FOR A LIVING

If you run IT for a Canadian organization, nothing about Thursday's announcement forces a switch. It does give you new leverage. Sovereignty is now an explicit federal priority with money behind it, which means "where does our data live and who can reach it" is a fair question to put to every AI vendor at renewal.

A practical approach for the next quarter:

1. **Map your sensitive workloads.** Separate the AI use cases that touch personal, health, financial or government data from the ones that don't. Only the first group needs a sovereignty conversation.
2. **Write residency into contracts, not just architecture diagrams.** Ask for data-location commitments, key ownership, and breach-notification timelines in writing.
3. **Keep a second model in reserve.** Whether it's Cohere, an open-weight model on your own hardware, or a Canadian-region deployment from a hyperscaler, a tested fallback is your best protection against price changes, outages or policy shifts.
4. **Watch the Regional AI Initiative.** If you're a small or mid-sized business in Southern Ontario, FedDev Ontario is one of the agencies delivering that $700 million. Adoption funding is often easier to win than research funding.



THE SOS TAKE

This is the right instinct with a few open questions. Backing a domestic AI company with equity instead of grants means taxpayers share the upside if Cohere succeeds, and the commitments are measurable. But sovereignty that only means "the servers are in Canada" won't be enough. The test will be whether Canadian buyers get real choice on price, capability and control. We'll be watching the first progress report and the November 5 federal budget for signs of whether Ottawa plans to buy what it just invested in.

READ THE ORIGINAL REPORTING // OPENS IN YOUR BROWSER

Prime Minister's Office: Cohere investment
pm.gc.ca ↗

Global News: Ottawa to invest up to $1.6B in Cohere
globalnews.ca ↗

PMO: National Council on Artificial Intelligence
pm.gc.ca ↗

CONNECTED // ALSO IN THE SOS FAMILY

OTTAWA'S COHERE STAKE
Sovereign stakes
SP&RTS · P.7 →

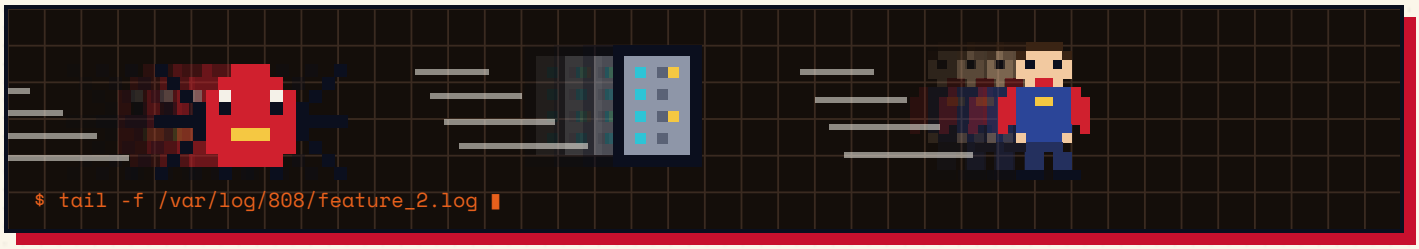
OTTAWA'S COHERE STAKE
The crawl
P&LITICS · P.12 →

OTTAWA'S COHERE STAKE
The crawl
CIRCUL&R · P.13 →

SOVEREIGN MONEY
Sovereign stakes
SP&RTS · P.7 →

$ PHP2SHELL IS THE PATCH YOUR WEB HOST OWES YOU THIS WEEK

Two critical bugs in PHP itself are being exploited, and a WordPress update won't save you



9.2
CVSS 4.0 score on both PHP2Shell flaws

2
critical remote code execution bugs

4 days
attacks before the patch shipped

25
servers rooted in one Oct 25 campaign

From BleepingComputer and The Hacker News.[4,6,11]

Every so often a vulnerability lands that isn't in an app or a plugin, but in the plumbing that runs a huge share of the web. PHP2Shell is one of those. If your company website, intranet, customer portal or WordPress site runs on PHP, which is most of the small-business web and a large share of shared hosting, you need to confirm it has been patched.

WHAT HAPPENED

On October 21, the PHP project shipped emergency, out-of-cycle releases to fix two critical remote code execution flaws, tracked as CVE-2026-109618 and CVE-2026-109619 and nicknamed "PHP2Shell." The PHP team scored both at 9.2 on the CVSS 4.0 scale.[4,12]

- **CVE-2026-109618** abuses the way PHP handles running out of memory. A carefully built request can leave PHP's internal data in a half-filled state, which attackers can turn into code execution.
- **CVE-2026-109619** is a use-after-free bug in PHP's upload-progress feature, the code that tracks file uploads.[13]

The detail that makes this nasty: both bugs trigger while PHP is parsing an incoming multipart form, *before* any of your own application code runs. Security firm GuidePoint put it plainly in its advisory: the parsing layer itself is the attack surface. A single unauthenticated request can be enough.[13,14]

THE TIMELINE WENT SIDEWAYS

According to a timeline published by Hostinger, researchers at the security firm Calif found the first flaw on August 1 while working under OpenAI's "Patch the Planet" initiative, and reported it to PHP on August 11. The plan was a coordinated release. Then, on October 20, the CVE numbers leaked before technical details were published, an exploit video was briefly posted and pulled, and a Hacker News post claiming to describe the bug was taken down.[5]

BleepingComputer reported that Amazon's threat intelligence team saw attackers targeting the flaws four days before patches shipped. CISA has since confirmed exploitation and ordered U.S. federal agencies to patch.[11] The Hacker News reported on October 28 that a suspected China-linked group used

an AI-assisted PHP2Shell exploit chain, paired with a Linux privilege-escalation bug, to root 25 servers on October 25, including three in a U.S. government-affiliated environment.[6]

Dark Reading compared the moment to Log4Shell, the Java logging bug that sent the industry scrambling nearly five years ago.[15] Tenable gave PHP2Shell its highest internal rating.[16]

WHICH VERSIONS ARE FIXED

The fixed upstream releases are **PHP 8.2.35, 8.3.36, 8.4.27 and 8.5.12**. Anything older on those branches is exposed.[12]

The harder news is for anyone running **PHP 8.1 or earlier**. Those branches are end-of-life, and there will be no official fix.[13] If a legacy site is still on PHP 7.x or 8.0, the only safe options are to upgrade it, isolate it, or take it down.

There's also a third, newer bug. PHP shared a mitigation for **CVE-2026-115560**, a separate remote code execution flaw that has no patch yet and only affects systems with what the PHP team called an unusual combination of configuration and application code. As of October 26, it wasn't in CISA's Known Exploited Vulnerabilities catalogue.[5,11]

WHAT TO DO TODAY

1. **Find every PHP runtime you own.** Run `php -v` on servers you manage. Check containers, old staging boxes and that marketing microsite nobody remembers launching.
2. **If you're on shared hosting, check your control panel.** On cPanel hosts, the MultiPHP Manager shows which PHP version each site uses. Confirm your host has rolled out patched builds, and if you can't tell, open a ticket and ask in writing. As Eye Security's Vaisha Bernard told ITdaily, this isn't something you can fix by updating WordPress or plugins, because the flaw is in PHP itself.[14]
3. **Use the stopgap only as a stopgap.** Before patches were available, PHP's guidance was to set `session.upload_progress.enabled=0` to block one attack path. It doesn't replace the update.[11]
4. **Assume compromise on anything that was exposed and unpatched.** Look for new admin users, unfamiliar files in upload directories, and odd outbound connections. Rotate database passwords and API keys stored in config files, because code execution through PHP usually means the attacker can read them.

Is your PHP safe? Fixed upstream releases

Branch	Fixed in	Status
PHP 8.5	8.5.12	☑ Patch available
PHP 8.4	8.4.27	☑ Patch available
PHP 8.3	8.3.36	☑ Patch available
PHP 8.2	8.2.35	☑ Patch available
PHP 8.1 and older	None	☐ End of life: upgrade
CVE-2026-115560	None yet	⚀ Mitigation only

Fixed versions per Computingforgeeks; end-of-life note per GuidePoint.[12,13]

THE SOS TAKE

PHP2Shell is a reminder that "we're just a small website" isn't a security strategy. Shared-hosting customers often assume the host handles everything below the app. Sometimes it does. Sometimes it's a ticket that sits in a queue. The window between disclosure and exploitation has collapsed to days, and in this case attacks started before the patch existed. Put your hosting provider's patch status on your calendar this week, and if your business runs on a PHP version that no longer gets fixes, treat the upgrade as overdue maintenance, not a project to pencil in.

READ THE ORIGINAL REPORTING // OPENS IN YOUR BROWSER

BleepingComputer: PHP ships emergency patches
bleepingcomputer.com ↗

Computingforgeeks: check and patch PHP2Shell
computingforgeeks.com ↗

GuidePoint Security: Keep calm and patch PHP2Shell
guidepointsecurity.com ↗

SUPPLY CHAIN // AI GATEWAYS

[3/3] feature.run

$ YOUR AI PLUMBING IS NOW AN ATTACK SURFACE

LiteLLM was poisoned for the second time this year. Here's what AI gateways need to be treated like



1h44m
poisoned LiteLLM 1.107.0 live on PyPI

2nd
LiteLLM compromise of 2026

~95M
LiteLLM downloads a month

5x
Gartner: agent costs by 2028

From Newly, CSO Online and VentureBeat.[3,17,18,19]

If your company has moved past chatbot experiments, you probably have something sitting between your apps and the AI model providers. It handles API keys, picks which model answers which request, logs usage and keeps costs in check. That layer is now one of the most valuable targets in your environment, and October made that obvious.

WHAT HAPPENED ON OCTOBER 21

LiteLLM is one of the most widely used open-source AI gateways. It's a Python library and proxy that lets developers call dozens of model providers through one interface. Its popularity is the point: CSO Online put its downloads at roughly 95 million a month earlier this year.[18]

On October 21, attackers published a malicious **version 1.107.0** to the Python Package Index (PyPI) and pushed matching tainted Docker images tagged `v1.107.0`, `latest`, `main-latest` and `main-stable`. According to LiteLLM's own incident report, as summarized by several security firms, the poisoned PyPI release was live from 11:39 to 13:23 UTC.[3,20]

This time the attackers didn't upload a fake package from outside. Security write-ups describe stolen GitHub credentials being used to point LiteLLM's real release workflow at a lookalike repository. The official source tag stayed clean, but the packages built and shipped to users carried a credential stealer.[17,21]

The payload drops files (`cook.pth`, `cook.py` and `sitecustomize.py`) into the Python environment. Python loads those automatically every time an interpreter starts, even if the program never imports LiteLLM.[22] Then it goes hunting for secrets.

AND THIS WAS THE SECOND TIME

In March, two malicious LiteLLM releases, versions 1.82.7 and 1.82.8, sat on PyPI for about 40 minutes after an attacker used a stolen publishing token.[23] That earlier compromise has been linked to a poisoned security scanner in LiteLLM's build process. PyPI's incident report estimated about 119,000 downloads during that window, according to a comparison of the two incidents published by Newly. Datadog said on October 21 that no link between the two compromises had been established.[17]

LiteLLM says earlier versions and its private Enterprise build weren't affected in October.[17]

IT WASN'T THE ONLY ONE

October's incident trackers read like a list of developer tooling under siege: hijacked GitHub release downloads for OVHcloud's command-line tool, a potential exposure of environment variables at the hosting platform Railway, a breach at the deployment platform Zeabur using leaked plaintext credentials, and stolen management keys used against WordPress sites through the UpdraftCentral backup service.[24] The common thread is that attackers are going after the systems that *hold* everyone else's keys.

WHY AI GATEWAYS ARE TIER-ZERO NOW

An AI gateway, by design, holds API keys for every model provider you use, often your cloud credentials too, and sees every prompt and response that passes through it. If it's compromised, an attacker can rack up model bills on your account, read sensitive data in prompts, and pivot into your cloud.

The trend is also heading toward more autonomy, not less. Google announced on October 8 that its new Gemini enterprise agent gets its own workplace identity, complete with an email address.[25] IBM launched agent identity and access controls on October 27.[26] And according to VentureBeat, Gartner expects agent costs to rise fivefold by 2028 even as per-token prices fall, because agents make so many calls.[19] More calls, more keys, more spend flowing through one chokepoint.

For what it's worth, the market hasn't caught up. SoftwareReviews opened an AI Gateways category this year, and as of October 29, none of its ten listed products, LiteLLM included, has enough reviews to be scored.[27]

WHAT GOOD LOOKS LIKE

1. **Pin and verify.** Lock dependency versions with hashes, not just version numbers. Never deploy containers from mutable tags like `latest` in production.
2. **Mirror what you install.** Pull packages through a private registry that delays brand-new releases by a day or two. Most poisoned releases are caught within hours.
3. **Make keys short-lived and narrow.** One key per provider, per environment, with spending caps. Rotate automatically.
4. **Watch for startup hooks.** Unexpected `.pth` or `sitecustomize.py` files in a Python environment are a red flag worth an alert.
5. **Limit outbound traffic.** Your gateway should only talk to the model providers you use. Anything else is suspicious.
6. **If you ran 1.107.0 or the affected Docker tags on October 21,** follow LiteLLM's remediation steps and rotate cloud credentials, SSH keys and AI provider keys.[20]

LiteLLM, hacked twice: March vs October

	March 24	October 21
Bad versions	1.82.7, 1.82.8	1.107.0 + 4 Docker tags
How they got in	Stolen PyPI token	Stolen GitHub creds, real release pipeline
Time live	About 40 minutes	11:39 to 13:23 UTC
Payload	Credential stealer	Startup hooks that run on every Python start

Compiled from Newly, Security Arsenal and AI/TLDR.[17,22,23]

THE SOS TAKE

Open-source AI gateways are still the right call for many teams, because they give you choice and keep you out of single-vendor lock-in. But the tools that route your AI traffic deserve the same controls as your identity provider or your password vault. If your AI gateway is running on a developer's laptop config with long-lived keys and a `latest` tag, October was your free warning.

READ THE ORIGINAL REPORTING // OPENS IN YOUR BROWSER

CSO Online: Python package security in 2026
csoonline.com ↗

Cloudsmith: LiteLLM 1.107.0 compromised
cloudsmith.com ↗

Newly: LiteLLM 1.107.0, are you affected?
newly.app ↗

THE CRAWL

$ THIS MONTH'S OTHER STORIES

Everything else we tracked, each summarised in a few sentences. Tap any card to read the original story in your browser.

NO. 01 // THE CRAWL

BANK OF CANADA HIKES FOR THE FIRST TIME SINCE 2023

The policy rate rose a quarter point to 2.50% on October 28, driven by energy-led inflation.[28] Expect lenders and vendors with CAD-financed contracts to reprice.

READ IT ON STORIES.TD.COM ↗

NO. 02 // THE CRAWL

FEDERAL BUDGET LANDS NOVEMBER 5

Finance Minister François-Philippe Champagne tables Budget 2026 two days after the U.S. midterms.[29] Watch for AI adoption, digital infrastructure and procurement measures.

READ IT ON ADVISOR.CA ↗

NO. 03 // THE CRAWL

OPENAI CUT PRICES FOR AGENT WORKLOADS

Coverage of the GPT-6.1 Terra release cited a 50% API price cut for agentic computer-use workloads, and the model is available in Microsoft Foundry.[26]

READ IT ON AIAGENTSDIRECTORY.COM ↗

NO. 04 // THE CRAWL

GEMINI BECOMES AN AGENT

Google's October 8 launch lets Gemini plan and carry out multi-step work across business apps, delegating to subagents.[25]

READ IT ON TECHCRUNCH.COM ↗

NO. 05 // THE CRAWL

CAPCOM AND SONY SO-NET BREACHES

Capcom confirmed 11.7 million CAPCOM ID email addresses were exposed.[30] Sony disclosed a So-net breach of about 2.58 million records.[31]

READ IT ON PRIVACYGUIDES.ORG ↗

NO. 06 // THE CRAWL

DHS STAFF DATA LEAKED

TechCrunch reported personal work details of more than 40,000 U.S. Department of Homeland Security employees were published after an earlier breach.[32]

READ IT ON TECHCRUNCH.COM ↗

NO. 07 // THE CRAWL

TAILSCALE PATCHED "TAILWORM."

Version 1.104.4 shipped October 27 to fix access-control vulnerabilities researchers disclosed days earlier.[31]

READ IT ON UNOSECUR.COM ↗

NO. 08 // THE CRAWL

CLOUDERA EXPANDS ITS AI ECOSYSTEM

New partners include Mistral AI, VAST Data, Neo4j and Cartesia, announced at EVOLVE26 New York on October 27.[33]

READ IT ON GLOBENEWSWIRE.COM ↗

NO. 09 // THE CRAWL

BINANCE: ONE LAPTOP, $6.3 BILLION

Binance says the October 29 theft began with a compromised laptop that reached a service container able to submit withdrawals. About $6.3 billion moved in roughly 20 minutes.[34] The FBI attributes it to North Korea's TraderTraitor.[35]

READ IT ON NPR.ORG ↗

NO. 10 // THE CRAWL

Q3 CLOUD SCORECARD

Azure disclosed dollars for the first time: $33.2 billion, up 48%.[36] AWS grew 39.3% to $46 billion, its fastest in nearly five years.[37]

READ IT ON TECHCRUNCH.COM ↗

NO. 11 // THE CRAWL

ANTHROPIC FILES TO LIST AS ANT

Anthropic's public S-1, filed October 26, shows about $16.3 billion in first-half revenue against an $80.7 billion net loss, mostly non-cash.[38]

READ IT ON MARKETSCALE.COM ↗

NO. 12 // THE CRAWL

ONE OPT-OUT FOR AI TRAINING

Google, Microsoft, OpenAI and Anthropic will honour a single robots.txt signal that refuses generative-AI training, now drafted at the IETF.[39]

READ IT ON SILICONANGLE.COM ↗

NO. 13 // THE CRAWL

IGNITE, THEN RE:INVENT

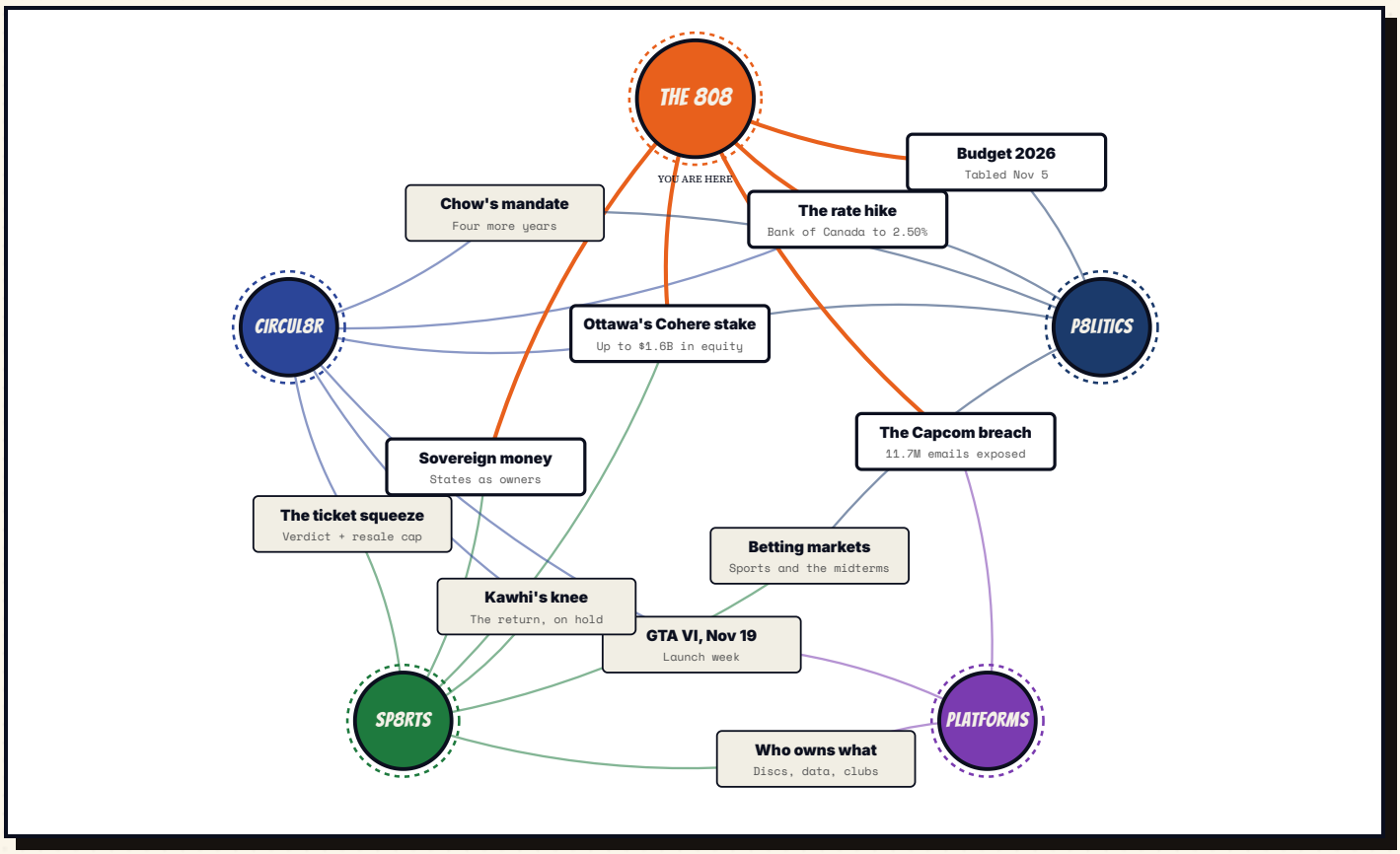
Microsoft Ignite runs November 17–20 in San Francisco with a free digital pass;[40] AWS re:Invent follows November 30 to December 4 in Las Vegas.[41]

READ IT ON MOSCONE.COM ↗

THE WIRE // CONNECTIONS

$ FIVE MAILERS, ONE MONTH

The same stories ran through all five of our mailers in October. Here is how they connect. Bold lines are this issue; tap a box or a chip to jump.



THE RATE HIKE

- P8LITICS · The Hormuz tax · p.4
- CIRCUL8R · The $100 night out · p.4
- CIRCUL8R · The crawl · p.13
- THE 808 · The crawl · p.13

OTTAWA'S COHERE STAKE

- THE 808 · Ottawa buys a seat at the AI table · p.4
- SP8RTS · Sovereign stakes · p.7
- P8LITICS · The crawl · p.12
- CIRCUL8R · The crawl · p.13

SOVEREIGN MONEY

- THE 808 · Ottawa buys a seat at the AI table · p.4
- SP8RTS · Sovereign stakes · p.7

THE TICKET SQUEEZE

- CIRCUL8R · The $100 night out · p.4
- CIRCUL8R · November, unwrapped · p.10
- SP8RTS · The crawl · p.12

BETTING MARKETS

- SP8RTS · The exchange will see you now · p.4
- P8LITICS · The crawl · p.12

GTA VI, NOV 19

- PLATFORMS · Eighteen days to Vice City · p.4
- CIRCUL8R · November, unwrapped · p.10
- CIRCUL8R · The crawl · p.13

KAWHI'S KNEE

- SP8RTS · The crawl · p.12
- CIRCUL8R · The crawl · p.13

THE CAPCOM BREACH

- THE 808 · The crawl · p.13
- PLATFORMS · The crawl · p.12

CHOW'S MANDATE

- CIRCUL8R · Four more years · p.7
- P8LITICS · The crawl · p.12

BUDGET 2026

- P8LITICS · Budget week · p.9
- THE 808 · The crawl · p.13

WHO OWNS WHAT

- PLATFORMS · Owning nothing · p.9
- SP8RTS · Sovereign stakes · p.7

CHECK OUR WORK

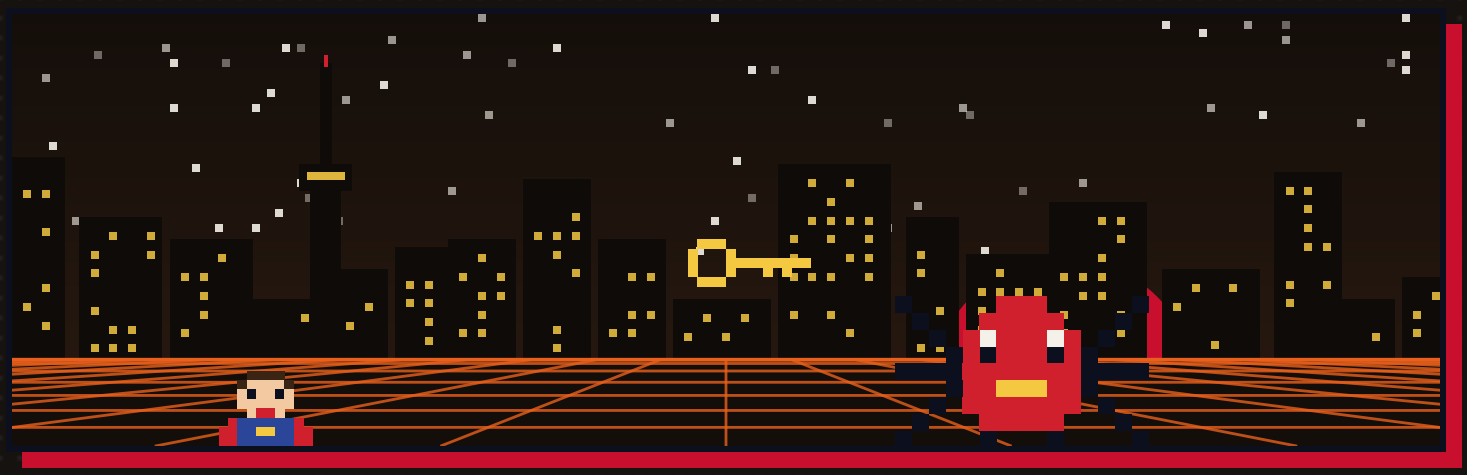
$ SOURCES

Every superscript number in this issue points here. In the PDF, each one is a link. 41 sources in all.

1. **Prime Minister's Office: Cohere investment**
   pm.gc.ca/en/news/news-releases/2026/10/29/canada-announces-landmark-investment-cohere-scale-secure-sovereign-ai
2. **Canada.ca / FedDev Ontario: Regional AI Initiative**
   canada.ca/en/economic-development-southern-ontario/news/2026/10/government-of-canada-expands-support-to-adopt-and-commercialize-artificial-intelligence.html
3. **Newly: LiteLLM 1.107.0, are you affected?**
   newly.app/security/litellm-compromise-for-ai-app-builders
4. **BleepingComputer: PHP ships emergency patches**
   bleepingcomputer.com/news/security/php-ships-emergency-patches-for-critical-php2shell-flaws
5. **Hostinger: php2shell timeline**
   hostinger.com/blog/what-is-php2shell/
6. **The Hacker News: PHP2Shell attack roots 25 servers**
   thehackernews.com/2026/10/php2shell-attack-roots-25-servers.html
7. **Global News: Ottawa to invest up to $1.6B in Cohere**
   globalnews.ca/news/12126174/ottawa-ai-investment-cohere/
8. **PMO: National Council on Artificial Intelligence**
   pm.gc.ca/en/news/news-releases/2026/10/02/prime-minister-carney-launches-new-national-council-artificial
9. **Open Canada: The human dimension of Canada's AI strategy**
   opencanada.org/the-human-dimension-of-canadas-ai-strategy/
10. **The Hill Times: Canada must chart its own AI future**
    hilltimes.com/2026/10/28/canada-must-chart-its-own-ai-future/522971/
11. **BleepingComputer: CISA confirms PHP2Shell exploited**
    bleepingcomputer.com/news/security/cisa-confirms-php2shell-vulnerabilities-now-exploited-in-attacks/amp/
12. **Computingforgeeks: check and patch PHP2Shell**
    computingforgeeks.com/php2shell-cve-2026-109618-check-patch/
13. **GuidePoint Security: Keep calm and patch PHP2Shell**
    guidepointsecurity.com/blog/how-to-patch-php2shell/
14. **ITdaily: PHP2Shell exploited ahead of patch**
    itdaily.com/blogs/software/php2shell-bug-php/
15. **Dark Reading: PHP2Shell red alert**
    darkreading.com/application-security/php2shell-bugs-red-alert-security-industry
16. **iTWire: Tenable on PHP2Shell**
    itwire.com/business-it-news/security/php2shell-the-14-year-old-bugs-that-pulled-cyber-gov-au-and-government-sites-worldwide-offline
17. **Newly: LiteLLM hacked twice, March vs October**
    newly.app/security/litellm-hacked-twice-march-vs-october
18. **CSO Online: Python package security in 2026**
    csoonline.com/article/4206245/python-package-security-in-2026.html
19. **VentureBeat: Gartner on agent costs**
    venturebeat.com/orchestration/gartner-says-agent-costs-will-rise-fivefold-by-2028-even-as-tokens-get-cheaper-here-is-how-to-keep-them-in-check
20. **Cloudsmith: LiteLLM 1.107.0 compromised**
    cloudsmith.com/blog/litellm-1-107-0-compromised-on-pypi
21. **TechJack Solutions: LiteLLM vendor rollup**
    techjacksolutions.com/scc-vendor-rollup/litellm-berriai-vulnerability-rollup-2026-10-22/
22. **AI/TLDR: LiteLLM 1.107.0 release note**
    ai-tldr.dev/releases/litellm-1-107-0-pypi-compromise/
23. **Security Arsenal: March LiteLLM releases**
    securityarsenal.com/blog/litellm-pypi-supply-chain-attack-2100-organizations-exposed-detection-hunt-queries-and-credential-rotation-guide
24. **Secucenter: Black October 2026 incident list**
    secucenter.com/blog/black-october-2026-biggest-cyberattacks-list/
25. **TechCrunch: Google brings agentic AI to Gemini**
    techcrunch.com/2026/10/08/google-brings-agentic-ai-to-gemini-starting-with-businesses/
26. **AI Agents Directory: news brief, Oct 27**
    aiagentsdirectory.com/news/ai-agents-news-brief-october-27-2026
27. **SoftwareReviews: AI Gateways category**
    softwarereviews.com/categories/ai-gateways
28. **TD Stories: Bank of Canada raises rate**
    stories.td.com/ca/en/article/bank-of-canada-interest-rate-october-2026
29. **Advisor.ca (CP): Budget on Nov. 5**
    advisor.ca/economy/liberals-to-table-2026-federal-budget-on-nov-5/
30. **Privacy Guides: breach roundup Oct 16–22**
    privacyguides.org/news/2026/10/23/data-breach-roundup-oct-16-22-2026/
31. **Unosecur: October 2026 incidents**
    unosecur.com/blog/october-2026-cybersecurity-incidents
32. **TechCrunch: DHS personnel data**
    techcrunch.com/2026/10/28/hacker-stole-personnel-data-about-thousands-of-homeland-security-employees-including-cbp-and-ice-agents
33. **GlobeNewswire: Cloudera AI ecosystem**
    globenewswire.com/news-release/2026/10/27/3388987/31982/en/cloudera-expands-enterprise-ai-ecosystem-to-power-ai-factories-anywhere.html
34. **NBC News: Binance targeted in $6.3B heist**
    nbcnews.com/business/markets/binance-hack-tether-circle-stablecoins-rcna606445
35. **NPR: Explainer on the $6.3B Binance heist**
    npr.org/2026/10/31/nx-s1-6024426/binance-crypto-heist-cyber-criminals-north-korea
36. **TechCrunch: Azure revenue $33.2B**
    techcrunch.com/2026/10/28/microsoft-just-shared-azures-actual-revenue-in-dollars-33-2-billion/
37. **Anadolu: Amazon Q3 2026**
    aa.com.tr/en/economy/amazon-net-sales-surge-12-to-202b-in-q3-as-cloud-unit-accelerates/4105482
38. **MarketScale: Anthropic files S-1**
    marketscale.com/industries/software-and-technology/anthropic-files-ipo-16-billion-six-month-revenue
39. **SiliconANGLE: AI crawling opt-out standard**
    siliconangle.com/2026/10/30/google-anthropic-and-others-to-support-new-ai-crawling-opt-out-standard
40. **Moscone Center: Microsoft Ignite 2026**
    moscone.com/node/852
41. **GovEvents: AWS re:Invent 2026**
    web.govevents.com/details/98147/aws-reinvent-2026

THE 808

THE 808 BRIEF // NOVEMBER 2026



NEXT MONTH

BUDGET 2026, FOR IT BUYERS.

Ottawa tables its budget November 5. Next month we read it for what matters to anyone buying AI, cloud and security in Canada.

Read it live at **the808.org**. Write to **contact@the808.org**.

CATCH US ON SOCIALS

@The808dotorg on X

FLIPBOOK // FRAME BY FRAME



THE 808 // THE 808

TO: TORONTO

Every reader, wherever you are.

A free monthly mailer. Independent, not affiliated with any team, party, company or government it covers. Cartoons are cartoons. Everything else is sourced.

The 808 · 621-38 Joe Shuster Way, Toronto, ON M6K 0A5 · contact@the808.org
You're receiving this because you subscribed at the808.org. To unsubscribe, reply "unsubscribe" or email contact@the808.org.