AI-ДАЙДЖЕСТ

Акції Anthropic виросли на 17% у перший день торгів

Ruby закрила діру з RCE у Rails, Java4Shell знайшли в PR від вересня, TSMC і Samsung зупинили поставки в Китай.

п'ятниця, 20 листопада 2026

У ЦЬОМУ ВИПУСКУ

1. Anthropic на біржі: +17% за перший день, ринок при цьому впав
2. Ruby закрила сім дір: одна дає захопити Rails-сервер без логіну
3. Java4Shell: та сама помилка два місяці лежала у відкритому PR
4. Чипи і Китай: TSMC і Samsung зупинили частину поставок, AMD упала на 11%
5. Білий дім замінив чиновника з кібербезпеки, а через підрядника витекли дані клієнтів Visa і JPMorgan
6. Суд у Британії: уряд мусить визнати таємний наказ Apple про доступ до шифрування
7. Gemini 4 Neon вийшла на перше місце в незалежному індексі, а на дизайн-бенчмарку лідирує анонімна модель
8. «Fuck your AI safeguards»: інженер не зміг закрити діру у власному сервісі через обмеження Claude [одне джерело]
9. Google з січня 2027 вимагатиме верифікації розробників для всіх Android-застосунків у світі [одне джерело]
10. Waymo прибрала роботаксі з автомагістралей у всіх містах США

ТЕМА 1

Anthropic на біржі: +17% за перший день, ринок при цьому впав

ДЖЕРЕЛА The Guardian, 19.11 Guardian · BBC, 19.11 BBC · Semafor, 19.11 Semafor · Platformer, 19.11 Platformer · @AnthropicAI, 19.11 @AnthropicAI · @TheRundownAI, 19.11 @TheRundownAI · HN Hacker News

Учора дайджест писав про ціну IPO: $83 за акцію. Сьогодні відомо, як пройшов перший день. Акції ANT відкрились на $111,50, тобто на 34% вище ціни розміщення. За даними BBC, максимум дня був $111,53, і тоді ринок оцінював компанію майже в $2 трлн. До закриття ціна впала до $97,17. Це плюс 17% до ціни IPO.

The Guardian рахує ринкову капіталізацію на закритті близько $1,3 трлн. З урахуванням усіх опціонів і обмежених акцій виходить $1,75-1,76 трлн, цю цифру дають і BBC, і Platformer. Разом з приватним розміщенням на $26 млрд Anthropic отримала $107,3 млрд, пише Semafor. Заявок на акції було приблизно вшестеро більше за пропозицію.

Решта ринку день не підтримала. За даними BBC, індекс Nasdaq Composite закрився на 2,3% нижче. Alphabet втратила 2,9%, Amazon майже 3,9%. Nvidia падає шостий день поспіль після свого звіту. The Guardian наводить цифри з проспекту:

виторг $16,2 млрд за перше півріччя 2026 року проти $4,6 млрд за весь 2025 рік. Збитки за дев'ять місяців 2026 року сягнули $104 млрд, і більшість з них дав одноразовий запис.

Даріо Амодеї у промові на Nasdaq пообіцяв «pace the training and deployment of AI systems, taking as long as is necessary». За даними Platformer, того ж дня понад 100 людей протестували біля офісу Anthropic у Сан-Франциско, і поліція затримала чотирьох за блокування входу. Platformer також нагадує вчорашній звіт METR: темп AI R&D в Anthropic приблизно подвоївся. За власною політикою безпеки компанії це вже поріг «Automated R&D».

Чому це важливо: уперше ринок дав щоденну ціну фронтир-лабораторії. Перший день показав дві речі одразу. Попит на саму компанію великий, але індекс техакцій від цього не виріс. Тепер кожен реліз і кожен інцидент Anthropic матиме біржову реакцію. Це новий канал тиску на темп роботи, і саме його згадують критики біля офісу.

ТЕМА 2

Ruby закрила сім дір: одна дає захопити Rails-сервер без логіну

ДЖЕРЕЛА Ruby, 18.11 Ruby-lang · Veria Labs, 20.11 Verialabs · @gdb, 19.11 @gdb · HN Hacker News · HN Hacker News

18.11 команда Ruby випустила версії 4.0.10, 3.4.13 і 3.3.14. Вони закривають сім вразливостей у рушії регулярних виразів і в зміні регістру рядків. Команда пише, що бачила робочі експлойти, і для частини дір це віддалене виконання коду. Ruby 3.2 і старші вже не підтримуються і виправлень не отримають.

Найгучніша діра має назву Ruby2Shell (CVE-2026-132825). Veria Labs пояснює механізм так. У більшості однобайтних кодувань німецька літера «ß» не має великої форми. Ruby при `upcase` пише замість неї два байти, «SS», а межу буфера перевіряє лише для одного. Буфер має запас у 20 байтів, тому рядок з 21 літерою «ß» переповнює його на один байт.

Помилка живе в коді з Ruby 2.4.0.

За даними Veria Labs, діра працює в Rails і Sinatra без жодних змін у налаштуваннях. Станом на 20.11 GitLab 19.6.0, GitHub Enterprise Server 3.22.5 і Chatwoot 4.20.0 ще не мають виправлених версій. Mastodon, OpenProject і Discourse уже оновились. Veria Labs обіцяє опублікувати робочий експлойт для Rails 25.11 або пізніше, якщо великі вендори не встигнуть.

Цю діру знайшли кілька команд незалежно. У бюлетені Ruby серед авторів стоять Stephan Lipp з Ada Logics разом з Anthropic. Veria Labs згадує ще Моріца Занфта, який працював разом з OpenAI. Грег Брокман подав це як «Codex for securing Ruby».

Чому це важливо: це четвертий такий випадок за місяць після PHP2Shell, Java4Shell і NGINX. Механізм щоразу однаковий: кілька команд з AI знаходять ту саму стару діру майже одночасно. Для команд з Ruby у проді є конкретна дата: до 25.11 треба оновити Ruby, а також усі продукти, що несуть власний Ruby всередині.

ТЕМА 3

Java4Shell: та сама помилка два місяці лежала у відкритому PR

ДЖЕРЕЛА OpenJDK PR #32781, 09.09 GitHub · Calif, 17.11 Calif · HN Hacker News

18.11 дайджест писав про Java4Shell, діру в декодері Base64 в OpenJDK. Calif показала її на рядку з 64 літер «A» і знака «=». 19.11 на HN підняли PR в OpenJDK від 09.09. Його автор, учасник проєкту, описує той самий код: декодер AVX-512 і той самий рядок `"A".repeat(64)+"="`. У PR прямо сказано, що стаб пише за межі буфера і пошкоджує купу.

PR чекав на рецензію. 04.11 бот попередив, що PR неактивний вісім тижнів, і того ж дня автор його закрив. На питання на GitHub він відповів 20.11: задачу взяли інші, у master цієї помилки вже нема. До PR ще у вересні вели звіти про падіння JVM з трекера Adoptium.

Чому це важливо: помилка пошкодження пам'яті була публічною за два місяці до розкриття як RCE. Тоді її бачили як рідкісне падіння на невалідному вводі, без оцінки наслідків. Зараз AI-інструменти швидко перетворюють такий опис на експлойт. Тому відкритий PR з фразою «corrupting the heap» варто читати як звіт про вразливість.

ТЕМА 4

Чипи і Китай: TSMC і Samsung зупинили частину поставок, AMD упала на 11%

ДЖЕРЕЛА Financial Times, 19.11 FT · Financial Times, 20.11 FT · Financial Times, 19.11 FT · Semafor, 19.11 Semafor · The Wall Street Journal, 20.11 WSJ

Скандал навколо Хуанга далі тягне весь ринок чипів. FT пише, що TSMC і Samsung призупинили частину поставок китайським клієнтам. Причина - нові експортні правила Міністерства торгівлі США. Другий матеріал FT: США раніше дозволили продаж чипів Nvidia і AMD китайським компаніям, які Пентагон вважає пов'язаними з армією Китаю.

Акції AMD 19.11 падали до 11% після звіту шорт-селера Hunterbrook. Звіт описує залежність AMD від китайського ринку і китайських поставок, а також фінансування власних клієнтів. AMD назвала звіт викривленням своїх практик. WSJ пише, що генпрокурор Каліфорнії Роб Бонта надіслав Nvidia слідчу повістку. Він перевіряє, чи не вводила компанія інвесторів в оману.

Чому це важливо: історія почалась з особистого скандалу одного CEO, а тепер змінює ланцюг поставок. Нові правила вже зупинили частину вантажів, і під перевірку потрапила вся галузь, разом з AMD. Для китайських AI-лабораторій це означає ще менше обчислювальних ресурсів на найближчі місяці.

ТЕМА 5

Білий дім замінив чиновника з кібербезпеки, а через підрядника витекли дані клієнтів Visa і JPMorgan

ДЖЕРЕЛА The Wall Street Journal, 20.11 WSJ · Semafor, 19.11 Semafor · HN Hacker News

17.11 дайджест цитував директора з кібербезпеки Білого дому Шона Кернкросса. Він тоді казав, що жоден з масових збоїв не був кібератакою. 20.11 WSJ пише, що Білий дім його замінив після збоїв. Подробиць за пейволом не видно.

Окремо Semafor пише про витік даних клієнтів Visa, Mastercard і JPMorgan. Хакери зламали стороннього постачальника послуг, це атака з вимаганням. Масштаб витоку станом на ранок 20.11 не названий.

Чому це важливо: збої після масових латок уже мають політичні наслідки: Білий дім замінив першого чиновника. Витік через підрядника нагадує, що навіть банк із найкращим захистом залежить від найслабшого постачальника в ланцюгу.

ТЕМА 6

Суд у Британії: уряд мусить визнати таємний наказ Apple про доступ до шифрування

ДЖЕРЕЛА Mac Anorak, 19.11 Macanorak · Financial Times, 19.11 FT · HN Hacker News

Трибунал з питань слідчих повноважень постановив 19.11, що уряд Британії мусить визнати факт наказу. Йдеться про Technical Capability Notice для Apple за законом Investigatory Powers Act 2016. Досі уряд не підтверджував і не спростовував наказ, хоча The Washington Post розповіла про нього ще в лютому 2025 року.

Через перший наказ Apple вимкнула Advanced Data Protection для нових користувачів у Британії. Під тиском США уряд відкликав перший наказ і видав другий, лише для британців. Трибунал написав, що уряд не довів шкоди для національної безпеки від визнання наказу. Законність самого наказу суд ще не оцінював.

Чому це важливо: таємність таких наказів трималась на правилі «не підтверджуємо і не спростовуємо». Тепер суд пробив це правило в одній справі, і розгляд по суті піде відкрито. Від нього залежить, чи може держава вимагати бекдор у наскрізному шифруванні.

ТЕМА 7

Gemini 4 Neon вийшла на перше місце в незалежному індексі, а на дизайн-бенчмарку лідирує анонімна модель

ДЖЕРЕЛА Models Engineering Index, 20.11 Github · micjm, 18.11 Micjm · Contra Labs, 18.11 Contralabs · @blader, 19.11 @blader · @blader, 19.11 @blader · HN Hacker News · HN Hacker News

18.11 Google випустила Gemini 4 Neon, і вчора всі цифри були з анонсу Google. Тепер є перші сторонні заміри. У Models Engineering Index Neon має 68,0 бала і стоїть першою. Claude Fable 5.2 має 65,3, GPT-6.2 Astra 61,5. За вартістю прогону індексу Neon обходиться в 1,6 умовних одиниці, Fable 5.2 у 6,4. Автор блогу micjm окремо оцінив Neon на своєму рейтингу Agent Duel приблизно на рівні Opus 5.5. Він рахує, що швидкість важить для користувачів майже стільки ж, скільки сама модель.

На дизайн-бенчмарку Contra Labs перше місце має анонімна модель Gestalt: Elo 1931 проти 1739 у людей-дизайнерів і 1713 у Fable 5.2. Під постом автора бенчмарку X повісив примітку спільноти. Там сказано, що Gestalt додав у таблицю сам творець бенчмарку і незалежної перевірки нема. Сікі Чен (@blader) пише, що Gestalt не від Anthropic, OpenAI, Google, xAI чи SSI, але звідки він це знає, не пояснює.

Чому це важливо: незалежний індекс поки підтверджує анонс Google, і ціна тут важить не менше за бали. Модель на рівні лідера, але вчетверо дешевша за прогін, міняє вибір для агентних задач. Результат Gestalt поки можна сприймати лише як заявку: таблицю веде та сама команда, що додала модель.

ТЕМА 8

«Fuck your AI safeguards»: інженер не зміг закрити діру у власному сервісі через обмеження Claude [одне джерело]

ДЖЕРЕЛА techtipsy, 19.11 Ounapuu · HN Hacker News

Автор блогу techtipsy, інженер з Естонії, попросив Claude Code пошукати прості проблеми з безпекою у власному продукті.

Claude знайшов одну помилку з виправленням в один рядок, а потім роботу зупинили захисні фільтри для кібербезпеки. Щоб отримати виняток, треба подати заявку, чекати кілька робочих днів, відмовитись від винятків щодо зберігання даних і надати документ з фото.

За словами автора, він закрив діру за допомогою відкритої моделі GLM 5.3 на європейському хостингу. На HN пост набрав 495 балів і понад 200 коментарів. Коментатори пишуть, що зловмисники обходять ці фільтри або беруть відкриті моделі, а захисники впираються в перевірку документів.

Чому це важливо: пункти 2 і 3 показують, як швидко AI знаходить діри. Цей пост показує зворотний бік: доступ до тих самих можливостей для захисту обмежений. Якщо легальний захисник іде до відкритих моделей без фільтрів, фільтри перестають

виконувати свою роботу. Компанії з власним кодом варто заздалегідь вирішити, якими моделями вони перевіряють безпеку.

ТЕМА 9

Google з січня 2027 вимагатиме верифікації розробників для всіх Android-застосунків у світі [одне джерело]

ДЖЕРЕЛА Ars Technica, 19.11 Ars Technica

Google почне вимагати верифікацію розробників у всіх регіонах з січня 2027 року. Після цього Android не встановить застосунок з будь-якого джерела, якщо розробник не зареєстрований у Google. Реєстрація вимагає державного документа і оплати $25. У вересні Google запустила систему в Бразилії, Індонезії, Сінгапурі і Таїланді.

Google каже, що вже зареєстровані «мільйони» застосунків поза Play, і це понад 99% встановлень у світі. Перевірка вже стоїть на сертифікованих пристроях з Android 8 і новіше. Galaxy Store, Xiaomi, Oppo, Vivo, Honor і Transsion показуватимуть лише перевірені застосунки.

Чому це важливо: вільне встановлення застосунків в Android закінчується. Для розробників поза Play це обов'язкова реєстрація з документом. Для анонімних і дрібних проєктів, наприклад open-source клієнтів, це новий бар'єр.

ТЕМА 10

Waymo прибрала роботаксі з автомагістралей у всіх містах США

ДЖЕРЕЛА The Guardian (AP), 19.11 Guardian · @TheRundownAI, 19.11 @TheRundownAI

Waymo на невизначений час зупинила комерційні поїздки автомагістралями в усіх містах, де вони були: Сан-Франциско, Лос-Анджелес, Фінікс, Маямі й Остін. Того ж дня DMV Каліфорнії заборонив роботаксі Waymo на автомагістралях штату.

Підстава - два інциденти. 05.11 три машини Waymo заїхали в зону ремонтних робіт. 06.11 одна з машин намагалась об'їхати патрульні машини, які зупиняли рух.

DMV назвав такі поїздки «imminent hazard to public safety». Тести на автомагістралях Waymo продовжує з водієм- спеціалістом за кермом. Поїздки міськими вулицями ця зупинка не зачіпає.

Чому це важливо: автомагістраль була наступним кроком для роботаксі, і регулятор зупинив його через повторні помилки в рідкісних сценаріях. Ремонтні зони і поліцейські перекриття трапляються рідко, але саме вони вирішують, чи дозволять автономному авто ширшу роботу.

misc

- **Claude і фізика чорних дір:** Anthropic 17.11 описала, як агенти Claude Fable 5.2 за шість тижнів розв'язали дві відкриті задачі квантової гравітації. Одна стосується фазового переходу Гокінга-Пейджа, друга дає точну межу для модульного бутстрапу. Результат перевірили в Lean, кожен головний результат перевірив фізик. На HN тема зібрала 428 балів 19.11. Anthropic · HN Hacker News
- **Профспілка в DeepMind:** працівники Google DeepMind у Британії об'єднуються в профспілку UTAW. Головна причина - військові контракти Google після того, як компанія прибрала заборону на AI для зброї. Co · HN Hacker News
- **МВФ про ставки:** Кристаліна Георгієва попередила, що попит на AI підніме процентні ставки в усьому світі.

  Guardian
- **Apple і агенти на Mac:** Bloomberg пише, що Apple наймає людей для агента, який сам керує комп'ютером. Марк Гурман пише, що в macOS 27.3 доступ стороннього агента ChatGPT до керування Mac тепер вимагає 14 кроків замість 4. @emollick чекає від цього роздратування клієнтів. @TheRundownAI · @emollick
- **Розумні окуляри:** нідерландський регулятор AP радить не купувати AI-окуляри. На тестах шести моделей одна кілька разів сказала, що викликала швидку, хоча не викликала.

  BBC
- **Шахрайство з токенами:** Клер Во з ChatPRD закриває безкоштовний пробний період. Групи крутили пробні акаунти і перепродавали доступ до її агента, серед них студія мап для Roblox і Fortnite.

  Simon Willison
- **PostgreSQL 19:** вийшов новий мажорний реліз PostgreSQL.

  Postgresql · HN Hacker News
- **Список AI-спамерів:** @levelsio опублікував список з 3 728 акаунтів X, які постять автоматичні AI-відповіді. 498 з них X уже заблокував. @levelsio