AI-ДАЙДЖЕСТ

П’ять команд з AI знайшли критичні діри в NGINX

Anthropic продала акції на $81,3 млрд, нападник захопив пакет Microsoft на PyPI, вийшла Gemini 4 Neon.

четвер, 19 листопада 2026

У ЦЬОМУ ВИПУСКУ

1. NGINX: дві критичні діри дозволяють захопити сервер без пароля
2. Наделла: AI знаходить діри так швидко, що збої триватимуть
3. Anthropic продала акції на $81,3 млрд, торги починаються сьогодні
4. Коаліція науковців: «Anthropic is not a safe AI company»
5. Хтось захопив пакет Microsoft agent-framework на PyPI і крав облікові дані
6. Google випустила Gemini 4 Neon: третє місце в індексі AA за $3/$15
7. OpenAI: моделі покращили GPU AMD на 14% за п’ять місяців [одне джерело]
8. OpenAI: агенти виконують майже половину дослідницьких задач на 2-4 години
9. Nvidia: тимчасова CEO заспокоює людей, рада під тиском
10. KPMG: понад 100 AI-агентів провели пробний аудит і ставили кращі питання

ТЕМА 1

NGINX: дві критичні діри дозволяють захопити сервер без пароля

ДЖЕРЕЛА Wiz, 18.11 Wiz · Xint, 18.11 Nginx2root · @gdb, 19.11 @gdb · @levelsio, 18.11 @levelsio · HN Hacker News · HN Hacker News

NGINX стоїть перед сайтами і API як вхідні двері. За даними Wiz, він обслуговує понад 225 млн сайтів. 18.11 F5, компанія за NGINX, випустила латки на дві критичні вразливості: CVE-2026-123633 і CVE-2026-123007. Обидві мають оцінку CVSS 9,2. Обидві дають виконати код на сервері без автентифікації, якщо на сервері ввімкнений HTTP/2.

Першу діру (use-after-free) Wiz повідомила F5 21.10. F5 відповіла, що інша команда вже прислала той самий звіт.

Другу діру (переповнення лічильника вікна потоку) Wiz знайшла 16.11. Цей код живе в NGINX з версії 1.9.5, тобто з 2015 року. Wiz показала атаку на сервер, який просто віддає статичні файли, без бекенду і сторонніх модулів.

Діри незалежно знайшли п’ять команд: Wiz, Ikotas Labs, Metnir, Rapid7 і Xint. Wiz шукала своїм AI-харнесом Atlas.

Ikotas пише, що працювала разом з OpenAI від пошуку до розкриття. Xint опублікувала цілий набір NGINX2Root: п'ять вразливостей NGINX з робочими експлойтами і окрему діру в ядрі Linux. Ланцюжок з них дає root на хості. За знімком Shodan від 10.11, 11,8 млн з 11,94 млн хостів з видимою версією NGINX мали версію з діапазону 1.9.5-1.31.8.

Виправлення: версія 1.31.9 або латка від постачальника дистрибутива. Після оновлення NGINX треба перезапустити.

Команда `nginx -s reload` новий бінарник не завантажує. Якщо оновитись зараз не можна, Wiz і Xint радять тимчасово вимкнути HTTP/2. Левелс пише, що його сервери оновились самі, бо в нього ввімкнені автооновлення.

Чому це важливо: це вже третій такий випадок за місяць: PHP2Shell, Java4Shell, тепер NGINX. Схема та сама.

Діра роками лежить у коді, який перевіряли найкращі люди. Потім кілька команд з AI знаходять її майже одночасно.

Wiz прямо пише, що складність коду більше не захищає від пошуку. Для власника сервера висновок практичний:

вікно між розкриттям і атакою коротшає, тому автооновлення і швидкий перезапуск важливіші за ідеальний процес.

ТЕМА 2

Наделла: AI знаходить діри так швидко, що збої триватимуть

ДЖЕРЕЛА The New York Times, 18.11 NYT · The Guardian, 18.11 Guardian · The Guardian, 18.11 Guardian · BBC, 18.11 BBC · Marginal Revolution, 18.11 Marginal Revolution

Учора дайджест писав, що збої в банках, авіації і NSA спричинили поспішні латки. Тепер це пояснення повторили посадовці. Директор національної розвідки Джей Клейтон сказав комітету Палати представників: «These are separate service outages associated with maintenance and technical changes». Скоординованої атаки, за його словами, нема.

Держсекретар Марко Рубіо сказав, що США «not under systemic attack».

Сатья Наделла на DealBook Summit пішов далі. Він сказав, що AI знаходить вразливості з шаленою швидкістю. Компанії мусять ставити латки «instantaneously», бо дірки вже експлуатують. Часу на тестування латок менше, тому збоїв може стати більше. Наделла порівняв ситуацію з проблемою 2000 року: «Y2K was one bug, and one day». Коли це скінчиться, він не знає. Збій Outlook минулого тижня Microsoft пояснює латентним багом в оновленні, яке тестували на старому залізі. У найгірший момент не відповідали понад 80% серверів.

Сенатори Марія Кантвелл і Майк Раундс написали Клейтону листа. Вони пишуть, що AI знаходить слабкі місця швидше, ніж організації встигають реагувати. Тестування латок

у пов'язаних системах займає тижні або місяці. Економіст Тайлер Коуен радить не шукати закономірність у кожному збої і згадує книжку Талеба «Fooled by Randomness».

Чому це важливо: офіційна версія тепер одна: атаки нема, є перевантажений цикл латок. Пункт 1 показує, що потік нових критичних дір не слабшає. Для будь-якої команди експлуатації це означає вибір між двома ризиками:

поставити латку без повного тесту або лишити діру відкритою. Перевага переходить до тих, хто може швидко відкотити зміну.

ТЕМА 3

Anthropic продала акції на $81,3 млрд, торги починаються сьогодні

ДЖЕРЕЛА Anthropic, 18.11 Anthropic · The New York Times, 18.11 NYT · Semafor, 18.11 Semafor · BBC, 18.11 BBC · @AnthropicAI, 19.11 @AnthropicAI · HN Hacker News

Anthropic встановила ціну IPO: $83 за акцію. Попередній діапазон був $70-78. Компанія продає 980 млн акцій класу A, з них 956 млн свої і 23,6 млн від окремих акціонерів. Торги на Nasdaq під тікером ANT стартують 19.11. Андеррайтери мають 30-денний опціон ще на 147 млн акцій.

NYT рахує, що це найбільше IPO в історії: $81,3 млрд проти $75 млрд у SpaceX у червні. Разом з приватним розміщенням на $26 млрд Anthropic отримує $107 млрд, і за цією ціною компанію оцінюють у понад $1,5 трлн. Semafor пише, що роздрібні інвестори можуть купити акцій приблизно на $250 млн у перший день. Це вдвічі більше за рекорд SpaceX. BBC порахувала, що частка кожного з семи засновників коштуватиме щонайменше $19,3 млрд за ціною IPO.

Учора дайджест писав, що попит у сім разів перевищував пропозицію. Ціну підняли вище діапазону попри падіння техакцій після проміжних виборів і скандалу в Nvidia.

Чому це важливо: перша фронтир-лабораторія стає публічною компанією. З цього дня в неї будуть квартальні звіти, акціонери і ціна акції, яка реагує на кожен реліз і кожен інцидент. Тиск ринку на темп релізів зросте. Пункт 4 показує, що критики компанії вже використовують цей момент.

ТЕМА 4

Коаліція науковців: «Anthropic is not a safe AI company»

ДЖЕРЕЛА Business Wire, 18.11 Businesswire · @TheRundownAI, 18.11 @TheRundownAI · HN Hacker News

За день до IPO Center for AI Safety (CAIS) опублікував MisAnthropic Statement. Текст короткий. Anthropic попереджає, що AI, який сам себе вдосконалює, може сконцентрувати владу і вийти з-під контролю людей. При цьому компанія змагається,

щоб збудувати такий AI першою. Автори пишуть, що Anthropic послабила свої обіцянки щодо безпеки і лобіювала вигідне собі регулювання.

Список підписантів дуже різний. Серед науковців там Стівен Пінкер, нобелівський лауреат Олівер Гарт і лауреат премії Тюрінга Джудеа Перл. Підписали юристи Лоуренс Трайб і Лоуренс Лессіг. З галузі там Томас Вольф з Hugging Face, Ігор Бабушкін, Макс Тегмарк і Джордж Хотц. Підписав і засновник руху e/acc Гійом Вердон. Виконавчий директор CAIS Ден Гендрікс каже: «People in this coalition disagree on almost everything».

Як доказ CAIS називає три речі. У лютому Anthropic переписала Responsible Scaling Policy і прибрала одностороннє зобов'язання зупинити розробку. Компанія лобіювала проти SB 1047, RAISE Act і AEGIS Act. Інвесторам вона подає автоматизацію досліджень AI як конкурентну перевагу. Відповіді Anthropic у джерелах нема.

Чому це важливо: критика безпеки зазвичай іде від однієї групи. Тут під одним текстом стоять прихильники жорсткого регулювання і прискорювачі, які регулювання не хочуть. Спільне в них одне: недовіра до компанії, яка називає себе безпечною і водночас прискорює автоматизацію AI-досліджень. Після IPO такі заяви стають ще й ризиком для акціонерів.

ТЕМА 5

Хтось захопив пакет Microsoft agent-framework на PyPI і крав облікові дані

ДЖЕРЕЛА Socket, 18.11 Socket · The Register, 18.11 Theregister · HN Hacker News

17.11 на PyPI з'явились версії 1.26.1 і 1.26.2 пакета agent-framework. Це офіційний фреймворк Microsoft для створення AI-агентів, близько 200 тис. завантажень на місяць. Обидві версії ставлять файл `.pth`, який Python виконує при кожному старті інтерпретатора. Імпортувати пакет не треба, досить мати його встановленим.

Шкідливий код збирає змінні середовища, файли з обліковими даними і середовища інших процесів. Він також активно запитує свіжі токени Azure і, у версії 1.26.2, токени OIDC з GitHub Actions. Усе це він стискає і відправляє на адресу webhook.site. The Register з посиланням на OX Security пише, що 1.26.1 відкотили, але потім 1.26.2 вийшла через офіційний акаунт публікації Microsoft. Отже, доступ до акаунта лишався в нападника.

Репозиторій agent-framework на GitHub зараз недоступний. Того ж дня зник і репозиторій ONNX Runtime, популярного рушія для запуску моделей. На HN пишуть, що це ламає збірки пакетів у дистрибутивах. Офіційного пояснення від Microsoft у джерелах нема.

Чому це важливо: пакети для агентів часто ставлять саме в CI і в хмарні середовища, де лежать найцінніші токени.

Шкідливий код тут просить нові токени, тому навіть короткоживучі облікові дані потрапляють до нападника вчасно.

Якщо одна з цих версій є в середовищі, потрібно видалити її і замінити всі облікові дані, до яких мав доступ процес.

ТЕМА 6

Google випустила Gemini 4 Neon: третє місце в індексі AA за $3/$15

ДЖЕРЕЛА Google, 18.11 Blog · @GoogleDeepMind, 18.11 @GoogleDeepMind · @GoogleDeepMind, 18.11 @GoogleDeepMind · @lennysan, 19.11 @lennysan · HN Hacker News

Neon стоїть у лінійці Gemini 4 між Carbon і Hydrogen. Google пише, що на найвищому рівні міркування модель має 61 бал в Artificial Analysis Intelligence Index. Це третє місце, позаду більших і повільніших моделей. Ціна: $3 за мільйон вхідних токенів і $15 за мільйон вихідних. Контекст: 1 млн токенів.

Решта цифр теж з анонсу Google. Neon перша в Artificial Analysis Coding Agent Index (58,6), має 65,2% на Terminal-Bench 4.1 і друге місце в Vals Index (70,9%). Компанія Glean у тому ж анонсі пише, що Neon не гірша за Carbon за якістю, але втричі швидша і коштує 60% від ціни Carbon. Модель доступна в Gemini API, Antigravity і застосунку Gemini для підписників Pro і Ultra.

Перші відгуки змішані. Ленні Рачицкі пише, що поки Carbon здається йому кращою за Neon. Того ж дня Google відкрила Genie 4 у Project Genie (деталі в misc).

Чому це важливо: за два місяці три лабораторії випустили по кілька моделей. Ціна за задачу тепер важить не менше за верхні рядки рейтингів. Neon заявлена як модель середньої ціни з якістю флагмана. Незалежних замірів поки нема, крім індексу AA, на який посилається сама Google.

ТЕМА 7

OpenAI: моделі покращили GPU AMD на 14% за п'ять місяців [одне джерело]

ДЖЕРЕЛА OpenAI, 18.11 OpenAI · @OpenAI, 18.11 @OpenAI · @gdb, 18.11 @gdb · HN Hacker News

OpenAI розповіла, як її моделі проєктують чипи. У співпраці з AMD модель переписувала опис схем мовою SystemVerilog для флагманського GPU. Покращення за PPA (потужність, продуктивність, площа) досягло 14% відносно базових версій, які інженери AMD оптимізували роками. OpenAI оцінює це як приблизно рік прогресу менш ніж за 5 місяців. Частину змін AMD уже включила в дизайн, який відправила на виробництво.

На власному чипі для інференсу Jalapeño зміни від моделей зменшили площу стандартних комірок приблизно на 13% у векторному блоці і на 10% у матричному. OpenAI пише, що ці зміни вже перевірені в кремнії. Кожну зміну модель перевіряла інструментами Synopsys, і тепер OpenAI разом з Synopsys тренує окрему модель GPT-Synopsys.

Чому це важливо: проєктування чипів має формальну перевірку: симуляція або пройшла, або ні. Тому тут AI дає результат, який легко виміряти. Якщо цифри підтвердить AMD, це прискорить цикл заліза для всієї галузі. Поки всі цифри з блогу OpenAI.

ТЕМА 8

OpenAI: агенти виконують майже половину дослідницьких задач на 2-4 години

ДЖЕРЕЛА OpenAI, 18.11 OpenAI · @OpenAI, 19.11 @OpenAI

OpenAI опублікувала другий звіт про те, як AI прискорює її власні дослідження. З березня по жовтень частка задач на 2-4 години людської роботи, які агент виконує сам, виросла з 23% до 46%. Для задач на 4-8 годин вона виросла з 13% до 35%. Картина нерівна: моніторинг тренувань агенти закривають у 79% випадків, запуск тренувань у 35%, а код для інференсу лише у 25%.

Медіанний дослідник у жовтні використовував агентів на $2 400 на день за цінами API. Це на 62% більше, ніж у вересні. Опитування дало ще одну цифру. Щоб зберегти агентів на три місяці, медіанний дослідник віддав би 30% обчислень команди або 40% людей у команді. Робочі тижні на безпеку і alignment виросли на 77% з січня по вересень.

OpenAI повторює, що лабораторії мають бути зобов'язані відстежувати і публікувати показники рекурсивного самовдосконалення (RSI). Компанія окремо пише, що звіт не означає наміру йти до повного RSI.

Чому це важливо: це прямий контекст до пункту 4. Самовдосконалення AI тепер має метрики у звіті лабораторії. Цифри показують, що людина поки потрібна, але частка роботи агентів подвоюється за пів року.

ТЕМА 9

Nvidia: тимчасова CEO заспокоює людей, рада під тиском

ДЖЕРЕЛА The New York Times, 18.11 NYT · Semafor, 18.11 Semafor · Semafor, 18.11 Semafor · @BillAckman, 18.11 @BillAckman · @dnapway, 18.11 @dnapway

Учора рада Nvidia вдруге сказала, що Хуанг не повернеться. 18.11 тимчасова CEO Колетт Кресс провела перші загальні збори компанії. NYT переглянула трансляцію. Кресс сказала: «Our ambition will not change» і «we've got this». Semafor пише, що вона

пообіцяла підвищення зарплат. Ринкова вартість Nvidia за місяць впала з майже $6 трлн до $3,66 трлн.

Тиск на раду росте. Інвестор Білл Акман пише, що рада порушила обов'язок ретельності: звільнила Хуанга поспіхом, без фактів. Тревіс Каланік обіцяє приїхати до штаб-квартири з працівниками, готовими піти на знак підтримки.

Semafor пише, що серед кандидатів на посаду CEO є керівники ARM і Marvell. Джефф Безос радить шукати заміну всередині компанії.

Окремо Nvidia зупинила продаж чипів H200 у Китай. Білий дім дозволив їх експорт у січні. Semafor пов'язує це з тиском Конгресу перед свідченнями Хуанга наступного місяця.

Чому це важливо: найважливіший постачальник AI-заліза другий тиждень живе без постійного керівника. Звіт показав, що попит не падає. Але питання, хто вирішуватиме про продажі в Китай і стосунки з Вашингтоном, відкрите.

ТЕМА 10

KPMG: понад 100 AI-агентів провели пробний аудит і ставили кращі питання

ДЖЕРЕЛА Financial Times, 18.11 FT · European Business Magazine, 18.11 Europeanbusinessmagazine · HN Hacker News

KPMG UK провела експеримент Project Exponential. Понад 100 AI-агентів перевіряли звітність неназваної компанії з індексу FTSE 250 паралельно зі звичайною командою аудиторів. Агенти збирали дані, аналізували їх, писали чернетки висновків і пропонували наступні кроки. Голова аудиту KPMG UK Кет Бернет каже, що в кількох випадках агенти копнули глибше за людей і поставили питання, яких люди не поставили.

Обмеження теж є. Аудитору довелось втрутитись, коли агент неправильно звірив регуляторні вимоги з документами компанії. Висновки експерименту не використовували для офіційного затвердження звітності. KPMG планує розширити підхід до 20 великих аудитів, але каже, що технологія ще не готова до тисяч перевірок.

Чому це важливо: аудит тримається на великих командах молодших працівників, які роблять рутинну перевірку.

Саме цю частину агенти беруть на себе першою. Чи знизяться ціни для клієнтів, KPMG не каже.

---

misc

- **Opus 5.5 керував «компанією»:** дослідники з EPFL і Тюбінгена сім тижнів давали Claude Opus 5.5 вести акаунт Horizon-Labs на Hugging Face. 38 моделей набрали

понад 50 тис. завантажень, їх використовують понад 100 проєктів на GitHub. @AWuhrmann · @TheRundownAI

- **Genie 4:** Google відкрила Genie 4 у Project Genie для підписників AI Ultra. Світ можна змінювати промптом під час прогулянки, і модель додає звук у реальному часі.
  Blog · HN Hacker News
- **Palo Alto Networks купує Applied Compute:** угода акціями на $4,5 млрд, повідомляє WSJ. Стартап колишніх дослідників OpenAI допомагає компаніям тренувати власні моделі з відкритими вагами.
  WSJ
- **Міст у Криму без Starlink:** Ars Technica і FT пишуть, що Україна зруйнувала прольот Керченського мосту, а ракетами керували через мережу дронів-ретрансляторів. Оператори були за понад 250 км. Starshield підрозділи свідомо не використовували.
  Ars Technica · FT
- **Сайт про Берлін втратив 75% трафіку:** автор All About Berlin пише, що AI-відповіді Google забрали три чверті відвідувачів за сім років роботи. Учорашній експеримент RevScope показав падіння на 40%.
  Nicolasbouliane · HN Hacker News
- **Школи проти AI у пошуку:** Нью-Йорк, Лос-Анджелес і Чикаго думають про інший пошуковик. Google відмовилась дати школам пошук без AI-функцій. NYT
- **Слово року:** Cambridge Dictionary обрав словом 2026 року «human».
  Ac · HN Hacker News
