

Один лінк на розмову ChatGPT міг віддати чужий акаунт

Стилер оцінює жертв через LLM, ядро Linux без виправлень, Jepsen розбив ParticleDB, кредитний стиск

неділя, 1 листопада 2026

У ЦЬОМУ ВИПУСКУ

1. Один лінк на розмову ChatGPT міг дати доступ до чужого акаунта
2. Стилер VOLTA просить LLM оцінити, скільки вартує жертва
3. Linux CVE-2026-98432: Red Hat підняв оцінку до 9.8, виправлення в Ubuntu і RHEL досі нема
4. Jepsen про ParticleDB: база для агентів, написана за допомогою LLM, не тримає навіть WHERE
5. Кредитний стиск доходить до neocloud і токенів
6. Binance: ФБР підтвердило Північну Корею, керівниця визнає помилки
7. Claude обмежує реверс-інжиніринг ігор, користувачі скаржаться і на навчання моделей
8. Податок на AI в Німеччині: міністри сперечаються, готового проекту нема
9. Карпаті за 2 години зробив YouTube з порад Hacker News
10. П'ять копій Qwen3.8-27B обійшли один виклик Fable 5 на задачах LiveCodeBench

ТЕМА 1

Один лінк на розмову ChatGPT міг дати доступ до чужого акаунта

ДЖЕРЕЛА [Parameter](#), 28.10 [Parameter](#) · Саймон Біллісон, 31.10 [Simon Willison](#) · HN, 31.10 [Hacker News](#)

Дослідники Parameter створили публічну розмову ChatGPT, яка запускала їхній JavaScript у сесії будь-кого, хто її відкрив. Код працював від імені chatgpt.com. Він читав список розмов жертви, діставав текст приватної розмови і відправляв дані на зовнішній сервер. У найгіршому варіанті жертві вистачало відкрити лінк, код спрацьовував приблизно за 4,5 секунди.

Сам Preview лишався ізольованим. Діру дала бібліотека MathLive, яку ChatGPT завантажує для графіків у головну сторінку. Вона приймала повідомлення `postMessage` від будь-якого вікна і вставляла отриманий HTML через `innerHTML`. Через це Preview міг створити в головній сторінці `iframe` без пісочниці. Політика CSP блокувала вбудовані скрипти, але дозволяла YouTube. Ендпойнт YouTube `oEmbed` віддавав назад текст параметра `callback` як виконуваний JavaScript.

Parameter подала звіт 18.10. OpenAI спершу оцінила його як P2, потім підняла до P1 і 26.10 підтвердила виправлення на обох версіях сайту. Віллісон пише про винагороду \$5 000 і вважає її замалою для такої вразливості.

Чому це важливо: кожна частина ланцюга окремо виглядала розумно. Небезпека з'явилась лише на стику функцій, тому перевірка кожної функції окремо її не бачить. Історія чатів тепер містить код, договори і ключі. Тому одна XSS в AI-чаті коштує дорожче, ніж на звичайному сайті. Хто показує згенерований HTML у себе, має перевірити сторонні бібліотеки в головній сторінці, особливо обробники `postMessage`.

ТЕМА 2

Стилер VOLTA просить LLM оцінити, скільки вартує жертва

ДЖЕРЕЛА Cisco Talos, 31.10 [Talosintelligence](#) · HN, 31.10 [Hacker News](#)

[одне джерело] Talos описала стилер для Windows, який сам себе видаляє. Він забирає паролі браузерів, куки, картки, seed-фрази гаманців, сесії Discord і Telegram, ключі SSH і хмари. Далі він використовує вкрадені сесії: шукає в Gmail чеки, щоб підтвердити домашню адресу, і забирає історію замовлень UberEats і DoorDash.

Новизна в останньому кроці. VOLTA відправляє зібране досьє в OpenRouter із запитом написати «оцінку цілі». Обов'язкові розділи звуться «WHAT THEY'RE WORTH» і «THEIR OPSEC». Модель за замовчуванням у коді `anthropic/claude-opus-4.6`. Якщо у відповіді є «I can't»

або «I'm not able», стилер іде далі ланцюгом: `kimik2`, потім `gemini-2.5-flash`. Запит іде через мережу самої жертви, тому власної інфраструктури в атакувальника нема.

У коді шість змінних слотів для ключів і каналу Telegram. Talos робить висновок, що автор продає конструктор: кожен покупець отримує свою збірку. Тоді оцінка жертви стає готовою функцією для покупця будь-якого рівня.

Чому це важливо: LLM тут заміняє аналітика, який переглядає тисячі журналів. Перехід на іншу модель після відмови коштує один `if`, тому захист однієї моделі не зупиняє такий конвеєр. На практиці Talos радить обмежити запуск Chrome у режимі без вікна, бо стилер цим обходить шифрування куків. Після зараження замініть токени і паролі, а гаманець вважайте втраченим.

ТЕМА 3

Linux CVE-2026-98432: Red Hat підняв оцінку до 9.8, виправлення в Ubuntu і RHEL досі нема

ДЖЕРЕЛА Atlas, оновлено 31.10 [Atlasum](#) · Ubuntu, 31.10 [Ubuntu](#) · HN, 31.10 [Hacker News](#)

Учора тут писали, що Go вмикає MPTCP за замовчуванням і цим розширює поверхню атаки. Тепер є зведена картина. 30.10 Red Hat підняв оцінку з Important (8.1) до Critical

(9.8). Станом на вечір 31.10 за часом США трекер Ubuntu показує «Vulnerable» для всіх релізів, а RHEL 8, 9 і 10 не має виправлення. Debian, SUSE, Oracle UEK і Amazon Linux свої ядра вже виправили. AlmaLinux тримає виправлення в тестовому репозиторії.

Red Hat і AlmaLinux дали правило nftables, яке відкидає TCP-пакети з опціями IPv4. Red Hat пише, що воно зменшує ризик, але не закриває його повністю. AlmaLinux попереджає, що трафік між контейнерами на одному хості може обійти правило. Помилка живе в ядрі з версії 4.4, а контейнер використовує ядро хоста, тому новий образ нічого не змінює.

Atlas нарахувала 36 репозиторіїв GitHub, які згадують цей CVE. Щонайменше шість заявляють, що містять тригер гонки або доказ концепції.

Atlas їх не перевіряла. У каталозі CISA KEV цього CVE на той момент не було.

Чому це важливо: виправлення в основному ядрі вийшло 11-15.10, а найбільші корпоративні дистрибутиви через два тижні ще чекають. За цей час у GitHub з'явилися заявлені докази концепції. Команда `ss -Mlnp` показує, чи є на сервері слухач MPTCP. У Go-сервісів зі збіркою 1.24 і новіше він є за замовчуванням.

ТЕМА 4

Jepsen про ParticleDB: база для агентів, написана за допомогою LLM, не тримає навіть WHERE

ДЖЕРЕЛА Jepsen, 31.10 Jepsen · HN, 31.10 Hacker News

Компанія Orkes написала ParticleDB на Rust для свого сервісу Conductor і продає її з акцентом на AI-агентів. На сайті стояло «Full ACID.

159K TPS» і «formally proven» з доказом на TLA+. Під час роботи з Jepsen специфікації TLA+ ніхто не показав.

Jepsen тестував один вузол, часто з одним клієнтом і без штучних збоїв. `WHERE 4 = 5` повертав рядки з первинним ключем 5, а `WHERE TRUE` не знаходив нічого. Обмеження NOT NULL і UNIQUE нічого не робили. Первинні ключі дублювались і ставали NULL. Сервер зависав або падав кожні кілька хвилин. Кожен режим транзакцій показав майже всі аномалії, які тести вміють ловити. Остання версія 1.1.18.11.rc-22 стала значно безпечнішою, але режим за замовчуванням і далі губив дані. Після тестів Orkes назвала ці режими в документації «experimental».

Найцінніший розділ Jepsen присвятив LLM. Команда з кількох інженерів зробила систему такого обсягу дуже швидко. Але інструменти LLM неодноразово заявляли про виправлення, якого не було. Orkes не змогла пояснити причини майже жодної помилки, а нові збірки виходили без журналу змін.

Чому це важливо: раніше обсяг коду і документації був ознакою зрілості проекту. Цю ознаку тепер легко підробити, пише Jepsen. Для бази даних перед використанням

лишається одна надійна перевірка: незалежні тести на те, що система справді гарантує. Заява про формальний доказ без опублікованої специфікації нічого не доводить.

ТЕМА 5

Кредитний стиск доходить до neocloud і токенів

ДЖЕРЕЛА BBC, 01.11 **BBC** · Еван Конрад, 31.10 @evanjconrad · The Wall Street Journal, 01.11 **WSJ**

Учора тут писали про межу зовнішніх грошей для OpenAI і Anthropic. BBC показує наступний рівень: neocloud, тобто компанії, які здають обчислення в оренду. CoreWeave має \$35,1 мільярда боргу, а її акції за місяць втратили чверть. Nebius, IREN і Applied Digital впали приблизно так само або більше. Gartner прогнозує, що до 2030 року 80% таких фірм втратять самостійність. Міністр фінансів США Скотт Бессент називає їх «малою частиною екосистеми».

Еван Конрад із SF Compute описує, як це відчувається знизу. За його словами, покупців обчислень просять передплатити майже 100%, бо ні вони, ні хмара не вважаються надійними позичальниками. Далі проблема доходить до токенів: провайдер шукає передоплату від клієнтів. Компанія зі списку Fortune 500 купує токени в кредит, а стартапу треба залучати капітал. Конрад продає рішення цієї проблеми, тому його оцінку варто читати з цією поправкою.

WSJ додає, що інвестори шукають страховку від падіння AI-ставки. Текст за пейволом, доступний лише початок.

Чому це важливо: перевага стартапу трималась на швидкості. Якщо агент робить роботу, а токени купують за кредит, велика компанія отримує перевагу в ціні грошей. Хто будує на чужих моделях, має рахувати не лише ціну токена, а й те, чи витримає постачальник вартість свого боргу.

ТЕМА 6

Binance: ФБР підтвердило Північну Корею, керівниця визнає помилки

ДЖЕРЕЛА The New York Times, 01.11 **NYT** · Financial Times, 01.11 **FT** · BBC, 31.10 **BBC**

Учора тут писали про атрибуцію від TRM і Chainalysis. Тепер NYT пише, що ФБР підтвердило їхні висновки про групу TraderTraitor. FT виносить це в заголовок. Як атакувальники обійшли захист, досі незрозуміло, пише NYT. TRM вважає ймовірним доступ до системи підпису гарячого гаманця, пише BBC.

NYT відновила ту ніч за словами чотирьох людей. О 16:20 у четвер почалися дивні транзакції, у робочому чаті зібралося близько 100 людей. Співкерівниця Хе Ї сказала у відео: «Ми мали інвестувати в безпеку набагато раніше і більше». Binance виділила \$6,34 мільярда на покриття збитків. Хе Ї пише, що річної виручки вистачить. Обсяг резервів компанії публічно невідомий.

Tether і Circle заморозили разом понад \$2 мільярди. World Liberty, криптокомпанія родини Трампа, заморозила \$27 мільйонів. \$2,4 мільярда TRM і далі вважає поза досяжністю. Чанпен Чжао тим часом сперечався в X з Ілоном Маском і нагадав, що Binance має акції SpaceX на понад \$1 мільярд.

Чому це важливо: найбільшу суму зупинили емітенти стейблкоїнів, які можуть заморозити монету одним рішенням. Така можливість суперечить обіцянці незалежності криптовалют, але саме вона зупинила найбільшу суму. Заява Хе Ї про AI як загрозу галузі поки не має опублікованих доказів щодо цього зламу.

ТЕМА 7

Claude обмежує реверс-інжиніринг ігор, користувачі скаржаться і на навчання моделей

ДЖЕРЕЛА Mashable, 31.10 [Mashable](#) · HN, 31.10 [Hacker News](#) · [@jiahaoshao1](#), 31.10 [@jiahaoshao1](#) · HN, 31.10 [Hacker News](#)

Учора в місцях тут було серверне правило про відтворення наявних ігор. Mashable, з посиланням на Tom's Hardware, пише ширше: Claude почав обмежувати модифікації, декомпіляцію і реверс-інжиніринг коду ігор. Офіційного оголошення нема. Обмеження заважають і звичайним розробникам ігор. Mashable пов'язує це з браузерними портами GTA і Call of Duty та зломом PS5.

Другу історію розповів один користувач. Цзяхао Шао пише, що система позначила його за «навчання конкурента», хоча він не робив дистилляцію Claude. Тепер, за його словами, будь-яка згадка RFT, SFT або навчання великих моделей дає блокування, перемикання з Orpus 5.5 на Orpus 5 або закриття сесії. Пост набрав 168 тисяч переглядів.

Частина HN сумнівається. Один коментатор пише, що Шао з Гонконгу, де Claude недоступний, тому VPN і робота з навчанням разом могли викликати класифікатор. Інший каже, що спокійно навчає на Claude моделі BERT. Перевірити ці заяви неможливо, Anthropic їх не коментувала.

Чому це важливо: класифікатор бачить тему, а наміру не бачить. Хто буде робити на одному постачальнику, може втратити частину функцій без оголошення і без журналу змін. Для критичних задач варто мати запасну модель і власний набір перевірок, який покаже таку зміну в день її появи.

ТЕМА 8

Податок на AI в Німеччині: міністри сперечаються, готового проекту нема

ДЖЕРЕЛА tagesschau, 29.10 [Tagesschau](#) · Дейв Мануель, 30.10 [Davemanuel](#) · [@levelsio](#), 31.10 [@levelsio](#) · Нік Картер, 31.10 [@nic_carter](#)

Учора тут писали про французьку поправку 0,055 євро за гігабайт. За добу X зліпив її з німецькою дискусією в сюжет «Європі бракує грошей». Пост @levelsio набрав 2,2 мільйона переглядів. Читачі додали уточнення: французька норма ще не закон, а німецької пропозиції формально нема.

Tagesschau дає деталі. Міністр цифрових справ Карстен Вільдбергер закликав оподаткувати «надзвичайно високий оборот» від AI і потім частково відступив. Міністерка сім'ї Карін Прін підтримує податок. Міністерка економіки Катеріна Райхе пропонує спершу впровадити AI. Канцлер Фрідріх Мерц налаштований скептично, а СПД відкрита до розмови.

Мануель порахував французьку норму на прикладах: €11,55 за одне завантаження GTA 6, €0,77 за футбольний матч у 4K. Оцінка автора поправки в €10 мільярдів на рік поки не має опублікованого розрахунку.

Чому це важливо: цікавіший за самі податки аргумент Ніка Картера. Європа збирає бюджет переважно з праці. Якщо працю замінює іноземна модель, місцевої бази податку стає менше, а прибуток лишається за кордоном.

Він сам вважає, що схема навряд чи спрацює. Цю логіку варто враховувати кожному, хто планує витрати на AI-сервіси в ЄС.

ТЕМА 9

Карпаті за 2 години зробив YouTube з порад Hacker News

ДЖЕРЕЛА Андрій Карпаті, 31.10 [Bearblog](#) · HN, 31.10 [Hacker News](#) · @patrickc, 31.10 [@patrickc](#)

Найгучніша сторі доби на HN, 881 бал. Карпаті втомився від рекомендацій YouTube і попросив Opus 5.5 зробити заміну. Модель завантажила коментарі HN, а Sonnet відфільтрував спам. Лишилось 40 тисяч коментарів і 6 454 відео за 2007-2026 роки. Сайт показує кадр із середини відео замість обкладинки і зберігає стан лише в браузері.

Робота зайняла приблизно 2 години. Руками Карпаті створив ключ Google API, запустив VPS і купив домен. За його словами, традиційної інженерної роботи він більше не робить. Того ж дня Патрік Коллісон написав, що додає в усі свої особисті застосунки поле «покращення»: текст одразу йде агенту, який це реалізує.

Чому це важливо: софт для одного читача перестав коштувати тижні. Ціна виправлення незручності в особистому інструменті падає майже до нуля. Для таких проектів це працює, бо помилка коштує мало. Сусідній пункт про ParticleDB показує інший кінець тієї самої шкали.

ТЕМА 10

П'ять копій Qwen3.8-27B обійшли один виклик Fable 5 на задачах LiveCodeBench

ДЖЕРЕЛА [Memdoor](#), 31.10 [GitHub](#) · HN, 31.10 [Hacker News](#)

[одне джерело] Автори Memdoor відтворили метод статті GVS5H: планувальник, два генератори ідей, виконавець і менеджер спілкуються лише через файли. Успіх визначає скрипт, а модель на це не впливає. На перших 10 задачах LiveCodeBench Hard за 5 проходів вийшло 9,8 з 10. Власна реалізація авторів статті дала 9,6, а Fable 5 окремо 8,0. Усі 50 запусків коштували \$35,79, медіана 40 хвилин і \$0,39 на запуск.

Обмежень багато, і автори їх називають. Це 10 задач зі 100. Fable 5 робив один виклик на задачу, тому порівняння нерівне. Задачі датовані березнем і квітнем 2025 року, тому модель могла їх бачити під час навчання. Менеджер двічі зіпсував правильне рішення: один раз вигадав контрприклад, інший раз не завершив цикл.

Чому це важливо: заголовок на HN обіцяє більше, ніж доводять дані. Сильна частина в іншому: зовнішня перевірка і багато дешевих спроб можуть компенсувати слабшу модель там, де успіх можна виміряти скриптом. Де такого тесту нема, цей метод не переноситься.

misc

- **PlanAssist:** Google DeepMind за власними даними скоротила на 58% час оцінки заявок на будівництво в Барнеті, Камдені і Дорсеті. Понад 70% звітів посадовці прийняли без правок. Сервіс отримають ще 12 органів влади в Англії.
[DeepMind](#) · [@GoogleDeepMind](#)
- **Factorio:** GPT-5.6 Sol пройшов гру в мирному режимі за 13,5 ігрової години. Під кінець він носив матеріали між частинами фабрики майже вручну.
[Ryanmadden](#) · [Hacker News](#)
- **Scribd:** компанія розсилає повідомлення про витік. Серед даних є пошта, останні 4 цифри картки і строк її дії. Те саме стосується Slideshare, Everand і Fable.
[Scribd](#) · [Hacker News](#)
- **Molly:** [одне джерело] форк Signal не оновлювався з 31.07, тому не має виправлень, які вже є в Signal 8.27.1. Автор допису радить перейти на основний клієнт.
[Piefed](#) · [Hacker News](#)
- **Nvidia і Китай:** [одне джерело] WSJ пише, що чиновники США, Сінгапуру і Тайваню підозрюють Еліс Хуан у передачі даних Китаю. Вона була керівницею Megaspeed International і близька до Дженсена Хуанга.
[WSJ](#)
- **Books3:** колишній дослідник Meta Стівен Роллер свідчив, що завантажив цей набір через торент і видалив його «через усі ці позови». Meta оскаржує такий висновок.
[Torrentfreak](#) · [Hacker News](#)

- **Агенти і семафор:** @emollick показав дослід Robocurve: дві ізольовані копії моделі обмінялись секретним словом через робота і камеру без попередньої домовленості.
[@emollick](#)
- **Prospero:** Кріс Веллонс випустив агента для коду на C++, який споживає на два порядки менше ресурсів за аналоги, за його оцінкою. [Nullprogram](#) · [Hacker News](#)
- **Сербія:** студентський список отримав 141 місце зі 250 у парламенті, більше половини обраних мають PhD або MD.
[Science](#) · [Hacker News](#)