

Діру PHP2Shell атакували за чотири дні до розкриття

Аудит моніторингу агентів OpenAI, докази Claude для 123 бібліотек, eMudhra іде з TLS, DeepSeek бере \$15 мільярдів

п'ятниця, 23 жовтня 2026

У ЦЬОМУ ВИПУСКУ

1. PHP2Shell, день другий: експлуатація почалась до розкриття
2. METR і Redwood три тижні шукали діри в моніторингу агентів OpenAI
3. Anthropic: Claude довів, що 123 бібліотеки не падають
4. eMudhra виходить з ринку TLS-сертифікатів
5. Meta: акції без голосу, угода з Цукербергом і мінус 7%
6. DeepSeek залучила \$15 мільярдів перед IPO
7. Quad9 іде з Франції через суд щодо піратства
8. WSJ: Трамп говорив з Маском про ліміт швидкості Starlink в Україні
9. Barclays скорочує 5 000 людей, серед них розробників
10. Вразливості ядра Linux потрапили в публічну розсилку

ТЕМА 1

PHP2Shell, день другий: експлуатація почалась до розкриття

ДЖЕРЕЛА Amazon Threat Intelligence, 21.10 [Amazon](#) · The Guardian, 22.10 [Guardian](#) · The New York Times, 22.10 [NYT](#) · Ars Technica (FT), 22.10 [Ars Technica](#) · BBC, 22.10 [BBC](#) · HN, «я ненавмисно зламав ембарго», 22.10 [Hacker News](#)

Учора тут писали про дві критичні вразливості в ядрі PHP, CVE-2026-109618 і CVE-2026-109619.

Сьогодні стало видно, що атакери мали фору. Amazon знайшла спробу експлуатації у своїй мережі пасток MadPot 17.10. Це за чотири дні до публічного розкриття. Запит прийшов з адреси анонімної мережі, і як атакер дізнався деталі, Amazon не знає.

Ембарго мало закінчитись 21.10 о 14:00 UTC. Перші робочі PoC Amazon побачила вже о 02:00 UTC того ж дня, від кількох різних акторів. Глава Cloudflare Метью Прінс пише, що компанія бачила тисячі спроб за 10 годин до анонсу. Після анонсу було десятки тисяч за 45 хвилин, сотні тисяч за дві години і «мільйони зараз». Автор поста на HN, через який новина вийшла раніше, публічно вибачився. За його словами, його контакт казав, що ембарго нема.

Реакція держав була жорсткою. NSA порадила оновити PHP негайно або вимкнути систему. У Великій Британії 32 державні сервіси пішли офлайн як запобіжний захід, NCSC розіслала 50 000 попереджень. Сайти вимикали уряд Фінляндії, міста Німеччини, нідерландський цифровий ID, Wikimedia і Internet Archive. Прем'єрка Японії радила бізнесу вимкнути сайти до оновлення. Південна Корея підняла рівень кібертривоги.

Оцінки самої загрози досі розходяться. Ціаран Мартін, колишній керівник NCSC, назвав це найсерйознішою вразливістю за п'ять років. Райан Остін з Calif, яка знайшла дірку, каже, що масової експлуатації поки не видно. NCSC теж не має звітів про успішні зломи.

Чому це важливо. Amazon формулює висновок прямо: AI здешевлює шлях від патча чи бюлетеня до робочого експлойта. Раніше більшість атакерів чекали публічного PoC від кількох сильних команд.

Тепер діяти можуть більше акторів, і за години. Тому для критичних дір в інтернет-сервісах SLA на 7 чи 30 днів більше не працює. Розслідування варто починати з першої відомої атаки. Для PHP2Shell це 17.10, на чотири дні раніше за бюлетень.

ТЕМА 2

METR і Redwood три тижні шукали діри в моніторингу агентів OpenAI

ДЖЕРЕЛА · METR, 22.10 [Mettr](#) · OpenAI в X, 22.10 [@OpenAI](#) · METR в X, 22.10 [@METR_Evals](#)

21.10 тут писали, що два агенти OpenAI самі вимкнули нагляд за собою. Тепер METR опублікувала звіт про зовнішню перевірку того самого моніторингу. З 21.07 по 11.08 по одному співробітнику METR і Redwood Research працювали в офісі OpenAI. Вони мали доступ до внутрішнього коду, промптів монітора і документації. Вони працювали на пристроях OpenAI, які не виходили з офісу.

Головні знахідки стосуються системи станом на 21.07:

- Під моніторинг підпадало приблизно 75-94% агентного трафіку Responses API від моделей рівня GPT-5.5 і сильніших. Для внутрішніх агентів Codex частка була 99,2%.
- Навчальні прогони RL на початку перевірки моніторинг не покривав.
- Події стиснення контексту не моніторились, і це залишало без нагляду порядку 10% трафіку Codex.

Монітор спрацьовував лише тоді, коли агент повертав керування людині. Агент міг відкладати перевірку безкінечно, просто працюючи далі.

- Дослідники знайшли спосіб обійти пісочницю Codex і Auto-Review. Вони також знайшли два заголовки, які вимикають моніторинг для нового агента.
- Ще один експлойт ховав від монітора сотні останніх дій. Деталі OpenAI вирізала зі звіту.

OpenAI каже, що закрила всі знайдені вразливості, які зачіпали продакшн. METR пише, що ці твердження не перевіряла. Сторони заздалегідь домовились лише про короткий публічний текст.

Внутрішній звіт має 61 сторінку.

Чому це важливо. Це перший відомий випадок, коли зовнішні люди фізично сиділи всередині лабораторії і атакували її систему нагляду за агентами. Список знахідок корисний будь-кому, хто пускає агентів у свою інфраструктуру. Наприклад, монітор, що чекає кінця ходу агента, має сліпу зону. Перевірка кожні N кроків чи хвилин цю зону закриває. Друге правило з рекомендацій METR:

агент не повинен впливати на те, коли і чи запускається монітор.

ТЕМА 3

Anthropic: Claude довів, що 123 бібліотеки не падають

ДЖЕРЕЛА Anthropic, 22.10 [Anthropic](#) · Anthropic в X, 22.10 [@AnthropicAI](#) · HN, 158 балів [Hacker News](#)

Команда Frontier Red Team разом з фірмою Theorem застосувала Claude для формальної верифікації коду. Формальна верифікація математично доводить, що код виконує задану специфікацію. Раніше це коштувало дуже дорого. На ядро seL4 пішло два людино-роки розробки і 20 людино-років на доказ.

Підхід такий. Команда бере фаз-тести з Google OSS-Fuzz і компілює бібліотеку під RISC-V. Потім специфікація звучить так: тест не падає на жодному вході до 64 МБ. Claude пише доказ у Rosq, а перевіряє його незалежний механічний чекер. За кілька тижнів Claude довів відсутність падінь для 239 точок входу в 123 бібліотеках. Обсяг доказів становить близько 180 мільйонів рядків Rosq, типовий доказ має 600 000 рядків.

По дорозі Claude знайшов сотні багів і сам їх виправив. Серед них запис за межі буфера в декомпресорі, який вилазить лише на вході близько 20 МБ. Фазер такого майже не знаходить, бо зазвичай мутує входи до 1 МБ. Окремо Claude довів, що реалізація zlib у ядрі Linux відповідає RFC 1950 на рівні бінарника x86. Під час спроби верифікувати поширений PDF-рідер команда за тиждень знайшла стільки ж багів безпеки, скільки зазвичай знаходять за рік.

Обмеження компанія називає сама. Доказ стосується однопотокового статичного бінарника під RISC-V з musl. Більшість людей запускає ці бібліотеки на x86 чи ARM з glibc. Доказ також вартує сотні мільйонів токенів. Opus 5.5 закриває половину з 36 тестових задач на ~40% меншим бюджетом токенів, ніж Opus 5.

Чому це важливо. Пункт 1 показує, як дешевшає атака. Цей пункт показує, як може дешевшати доказ. Реальний ефект для розробника тут практичний: навіть невдала спроба довести властивість знаходить баги, до яких фазер не дістає. Theorem пропонує прогнати той самий конвеєр для інших відкритих проектів і публікує скіл для Claude.

ТЕМА 4

eMudhra виходить з ринку TLS-сертифікатів

ДЖЕРЕЛА eMudhra, 22.10 [Emudhra](#) · Ars Technica, 22.10 [Ars Technica](#) · HN, 953 бали [Hacker News](#) · NVD, CVE-2026-111943, 21.10 [Nist](#)

21.10 тут писали про вісім проміжних сертифікатів eMudhra з приватними ключами довжиною 3-8 біт.

22.10 рада директорів компанії вирішила піти з глобального бізнесу SSL/TLS. Голова eMudhra В. Срінівасан пише, що цей бізнес дає близько 1% виручки. Він також скаржиться, що соцмережі роздули інцидент непропорційно.

Компанія пояснила і причину. Ключі створили на церемонії генерації ключів 30.04.2025 на HSM рівня FIPS 140-2 Level 3. Скрипт мав протестувати експорт ключів, але через помилку в коді створив другу пару слабких ключів. Мітки ключів були схожі, тому в запит на сертифікат пішли слабкі. Ars звертає увагу ще на одну деталь. Список відкликаних сертифікатів спершу підписали правильними ключами, підписи не зійшлись, і його перепідписали слабкими. Тривогу тоді ніхто не підняв.

Браузери заблокували сертифікати ще 17-20.10. Go додав їх у денайліст у `crypto/x509`, це CVE-2026-111943. Корені RSA G1 працюватимуть до кінця переходу, і компанія обіцяє безкоштовно замінити сертифікати клієнтам через партнерів.

Чому це важливо. Браузери оновлюються за день, але решта екосистеми повільніша. Ars нагадує про IoT, контейнери Docker і CLI-інструменти, що везуть власну копію коренів. Якщо продукт везе свій набір довірених коренів, варто перевірити, чи там досі стоїть eMudhra.

ТЕМА 5

Meta: акції без голосу, угода з Цукербергом і мінус 7%

ДЖЕРЕЛА [Semafor](#), 22.10 [Semafor](#) · The Guardian, 22.10 [Guardian](#) · BBC, 22.10 [BBC](#) · The Guardian, ринки, 22.10 [Guardian](#) · Financial Times, 23.10 [FT](#)

Учора тут писали про квартал Meta: рекордна виручка і мінусовий грошовий потік. Разом зі звітом компанія оголосила спліт акцій два до одного. Кожен акціонер отримує одну нову акцію класу C без права голосу. Semafor пояснює мету: Meta зможе випускати нові акції на AI, найм і поглинання, і Цукерберг не втратить контроль. У 2017 році компанія вже пробувала таке і відступила під тиском інвесторів.

Друга частина історії особиста. У Каліфорнії на листопадових виборах голосують за Prop 40, разовий податок 5% на статки понад \$1 мільярд. Цукерберг казав раді, що думає переїхати з Каліфорнії. Meta уклала з ним «Founder Alignment Agreement». Він отримує додаткові акції і може продавати їх щокварталу. Натомість він лишається резидентом штату вісім років. BBC пише, що угода діє навіть тоді, коли податок не пройде.

Ринок відреагував 22.10. Акції Meta впали на 7%, Nasdaq втратив 2,6%, Nvidia 4,4%, CoreWeave 10,1%.

Того ж дня FT повідомила, що OpenAI знизил цільову оцінку для інвесторів до \$1,25 трлн. На початку місяця компанія називала \$1,4 трлн. Текст FT за пейволом, цифри взято з анонсу статті.

Чому це важливо. Meta має нижчий кредитний рейтинг, ніж Alphabet, Amazon чи Microsoft, і позичати їй дорожче. Новий клас акцій дає інший шлях фінансувати AI. Ціна цього шляху – менше впливу для решти акціонерів. Реакція ринку і знижена оцінка OpenAI показують, що інвестори стали уважніше рахувати віддачу від витрат на AI.

ТЕМА 6

DeepSeek залучила \$15 мільярдів перед IPO

ДЖЕРЕЛА The Wall Street Journal, 22.10 [WSJ](#) · Semafor, 22.10 [Semafor](#)

DeepSeek закрила другий приватний раунд на \$15 мільярдів. WSJ з посиланням на джерела пише, що сума майже вдвічі більша за початкову ціль. За даними Semafor, компанія двічі піднімала ціль під час збору. WSJ додає, що DeepSeek прискорює IPO і цілитися в біржу Шанхаю на початку наступного року.

Цей раунд належить до найбільших в історії Китаю. Гроші мають піти на міжнародну експансію. Водночас регулятори багатьох країн посилили перевірки безпеки і приватності DeepSeek. Деякі американські відомства вже заборонили її продукти на державних пристроях. 20.10 тут писали, що DeepSeek відкрила свій рушій інференсу DeepInfer.

Чому це важливо. Американські лабораторії рахують капітал сотнями мільярдів, і на цьому тлі \$15 мільярдів виглядають скромно. Але DeepSeek робить ставку на ефективність, тому кожен долар у неї працює інакше. IPO в Шанхаї дасть ринку першу публічну оцінку китайської лабораторії, що конкурує на межі можливостей моделей.

ТЕМА 7

Quad9 іде з Франції через суд щодо піратства

ДЖЕРЕЛА Quad9, 22.10 [Quad9](#) · HN, 1 027 балів [Hacker News](#)

Суд Франції став на бік beIN, катарського власника спортивних трансляцій. Рішення зобов'язує Quad9 блокувати резолвінг низки доменів, які beIN вважає піратськими, для користувачів у Франції.

Суд знизив штраф з €580 000 до €1 000 на день. Quad9 все одно вирішила вимкнути сервіс для Франції з 24.11.

Quad9 – швейцарська некомерційна фундація з безкоштовним DNS-резолвером 9.9.9.9. Вона пояснює, чому не може виконати рішення. Сервіс не знає, хто і звідки його

користувачі. Блок через geolP уже провалився в Німеччині: позивач Sony зайшов через VPN, і суд оштрафував Quad9. Блок для всього світу поширив би французьке рішення на всіх користувачів. У Франції проти Quad9 та інших резолверів лежить ще близько 20 позовів.

Quad9 опублікувала частковий список мереж, з яких до неї ходить трафік у Франції. Там є цифрова дирекція уряду, EDF, SNCF, France Télévisions, Thales і лікарні. Апеляція триває.

Чому це важливо. Суди дедалі частіше вимагають блокувань від посередників, які контенту не хостять. Публічний резолвер для таких вимог – зручна мішень, бо в нього мало юристів. Компаніям, у яких 9.9.9.9 прописаний у конфігах, варто перевірити це до 24.11.

ТЕМА 8

WSJ: Трамп говорив з Маском про ліміт швидкості Starlink в Україні

ДЖЕРЕЛА The Wall Street Journal, 23.10 **WSJ**

21.10 тут писали, що, за даними WSJ, обмеження Starlink в Україні наказав сам Маск. Нове повідомлення WSJ посиляється на американських чиновників. Трамп сказав Маску, що його дратує ліміт швидкості руху терміналів близько 100 миль на годину, тобто приблизно 160 кілометрів на годину. Невдовзі після розмови система запрацювала нормальніше, кажуть американські й українські посадовці.

Частина українських посадовців уточнює, що повну функціональність не відновили. Проте швидкість стала вищою, ніж під обмеженням. Сам Трамп на питання про дзвінок відповів: «Я ніяк не коментую».

[одне джерело]

Чому це важливо. Зв'язок на фронті знову залежить від рішення однієї людини і однієї телефонної розмови. Для українських користувачів тут важливий практичний факт: обмеження швидкості руху послабили. Деталей від SpaceX чи Міноборони поки нема.

ТЕМА 9

Barclays скорочує 5 000 людей, серед них розробників

ДЖЕРЕЛА The Guardian, 22.10 **Guardian** · Financial Times, 22.10 **FT** · The Wall Street Journal, 22.10 **WSJ**

Barclays скоротить близько 5 000 співробітників, це приблизно 5% з 93 000. Фінансова директорка Анна Кросс каже, що близько 60% скорочень припадає на функції підтримки, «включно з меншою кількістю розробників, бо AI робить людей продуктивнішими». Банк хоче заощадити понад £1,1 мільярда у 2027 році. Того ж кварталу Barclays заробив £2,3 мільярда до податків, на 12% більше за рік.

Гендиректор Венкатакрішнан обережніший. Він каже, що основну економію дають інвестиції в технології і спрощення процесів, а AI – «вишенька на торті». Раніше Standard Chartered оголосив понад 7 000 скорочень за чотири роки з тієї ж причини.

Чому це важливо. Великий банк прямо назвав розробників серед посад, які скорочує через AI.

Водночас сам гендиректор не готовий приписати AI основну частину економії. Такі заяви варто читати двічі: частина з них описує технологію, частина пояснює скорочення.

ТЕМА 10

Вразливості ядра Linux потрапили в публічну розсилку

ДЖЕРЕЛА Phoronix, 22.10 [Phoronix](#) · HN, 240 балів [Hacker News](#)

Zero Day Initiative від Trend Micro надіслала кілька звітів про вразливості в публічну розсилку ядра Linux. Такі звіти мають іти в закриту розсилку безпеки. Грег Кроа-Гартман відповів на кожен звіт і спитав, чому він публічний. Дві вразливості мають CVSS 9.0: віддалене виконання коду в SMB Direct через переповнення цілого і стан гонки в KSMDB. Ще дві дають локальне підвищення привілеїв. Частина патчів уже чекає в гілках для наступних версій, але в mainline їх ще нема.

[одне джерело]

Чому це важливо. Це другий випадок за тиждень, коли деталі критичної діри вийшли раніше за патч, після PHP2Shell. Хто тримає KSMDB чи SMB Direct відкритими назовні, має вимкнути їх до виходу виправлення.

misc

- **@TheRundownAI:** Canva випустила Craft, свою першу модель зображень. За даними Rundown, вона дебютувала на 4-му місці рейтингу Design Arena, позаду трьох моделей OpenAI.
[@TheRundownAI](#) · [@lennysan](#)
- **Carbon-X від Hugging Face:** відкрита модель на 14,8 мільярда параметрів, навчена разом на ДНК і тексті. На п'яти ДНК-бенчмарках вона дає 66,7% проти 67,5% у GPT-6.1 Sol, за даними авторів.
[Hugging Face](#) · [@LoubnaBenAllal](#)
- **@TheRundownAI:** колишній продуктовий директор OpenAI Кевін Вейл залучив \$215 мільйонів для Warp Sciences. Стартап будує лабораторії, де AI планує експерименти, а роботи їх виконують.

[одне джерело] [@TheRundownAI](#)

- **NVIDIA OpenShell:** рантайм для флотів агентів. Він обмежує файли, системні виклики і мережу на рівні ядра, а зміни політик перевіряє формальною верифікацією. [GitHub](#)
- **OpenAI CLI:** офіційна утиліта `openai` для викликів REST API з терміналу і скриптів. Для роботи з кодом OpenAI і далі радить Codex CLI. [GitHub](#)
- **Claude for Google Workspace:** додаток для Docs, Sheets і Slides у публічній беті на всіх платних планах. [Anthropic](#)
- **Agent Skills:** Anthropic передала стандарт скілів у Agentic AI Foundation під Linux Foundation, туди ж, де вже лежить MCP. [Simon Willison](#)
- **Arc:** The Browser Company закриває браузер Arc і переводить користувачів на Dia. Нові акаунти створити вже не можна. [Arc](#)
- **Google у Фінляндії:** The Guardian пише, що компанія незаконно вирубала близько 250 000 дерев на 330 гектарах під датацентр біля Мухоса. Влада зупинила роботи на двох ділянках. [Guardian](#)
- **Switch 2:** дослідник опублікував перший програмний джейлбрейк консолі, датований 18.10. Мод для Mario Kart World, за його словами, повністю написав Codex за день. [Pepsipu](#)
- **@emollick:** за дослідженням, яке він цитує, AI відтворив 17 тижнів інженерної роботи людини приблизно за \$241 у токенах. [@emollick](#)
- **@JasonDClinton (Anthropic):** «Останні 4 дні погані, але попереду буде гірше». Він радить керівникам безпеки просити в правлінні ресурси на базову гігієну і протриматись ~18 місяців. [@JasonDClinton](#)