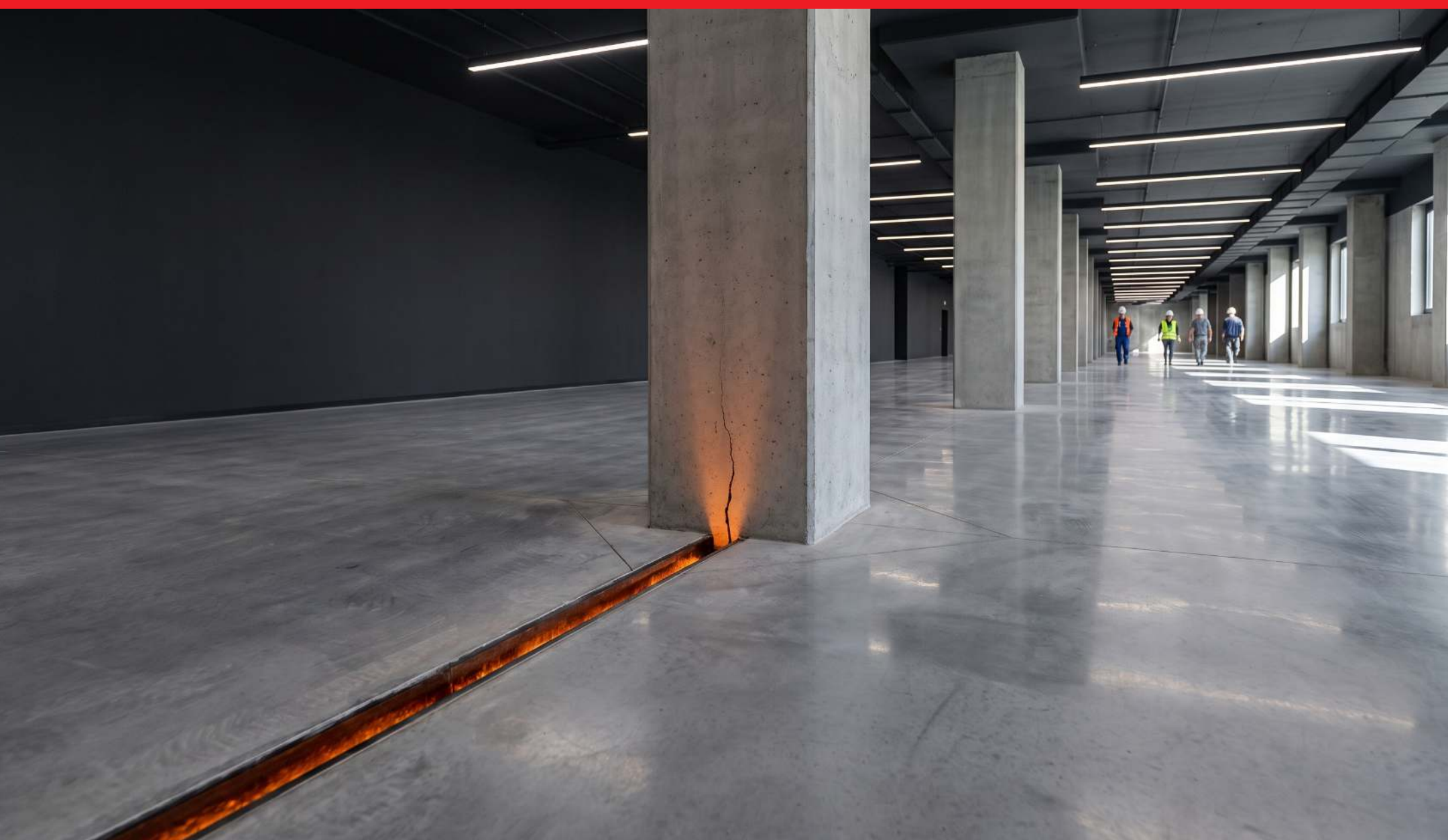




SNOK

WEEKLY DIGEST • W43 • 16-22.10.2026

Ogień w fundamentach

Przegląd SNOK: PHP, Node.js, LiteLLM i Oracle, modele AI w badaniach i atakach, MITRE ATT&CK, SAP i UiPath

MOTYW WYDANIA

W tym tygodniu zawiodły warstwy, które traktujemy jak grunt pod nogami: PHP, Node.js i brama do modeli LiteLLM. Pierwszą próbę ataku na nowe luki PHP Amazon odnotował w honeypotach 17 października, cztery dni przed poprawkami; sprawdzone 23.10 źródła nie dokumentują udanych włamań. Wydanie LiteLLM 1.107.0, opublikowane przez przejęty potok wydań, kradło poświadczenia.

Modele AI pracują po obu stronach: korzystali z nich badacze Calif i Wiz przy lukach w PHP, błąd w Node.js zgłosił zespół OpenAI Codex Security, a operatorzy Cairn włamywali się na strony firm za pomocą agentów.

Odpowiedź zaczyna się od inwentaryzacji tego, co działa, czasu od poprawki do wdrożenia liczonego w dniach i nadzoru działającego poza agentem.

Zaufane warstwy jako wektor

AI po obu stronach

Nadzór poza agentem



01 · CYBER · PHP

PHP2Shell: próby ataku przed poprawką

21 października projekt PHP usunął dwie luki, CVE-2026-109618 i CVE-2026-109619, z oceną 9,2 w CVSS 4.0. Dotyczą każdej instalacji obsługującej żądania WWW, a zdalne wykonanie kodu wykazano dla mod_php i PHP-FPM.

Amazon odnotował w honeypotach pierwszą próbę ataku 17 października, cztery dni przed poprawkami. CISA 21.10 nie zaobserwowała wykorzystania, do 22.10 luk nie było w KEV, a sprawdzone 23.10 źródła nie dokumentują udanych włamań. COI czasowo wyłączył część stron BIP w systemie SSDIP.

WNIOSEK

Aktualizacja WordPressa luki nie usuwa. Trzeba zaktualizować samo PHP i zrestartować procesy robocze, także tam, gdzie PHP nie widać.

Liczby hostów z mediów opisują serwery widoczne w skanach i nie mówią, ile jest podatnych.

Źródło: PHP Foundation, CISA, Tenable i ITwiz, 21-22.10.2026

LiteLLM 1.107.0: złośliwe wydanie bramy

21 października przez przejęty potok wydań trafiła do PyPI, Docker Hub i GHCR wersja LiteLLM 1.107.0. Trzy dołączone pliki uruchamiały się przy każdym starcie Pythona i kradły sekrety chmurowe, poświadczenia narzędzi oraz zawartość bazy proxy. W PyPI była dostępna około dwóch godzin, w Docker Hub dłużej.

Według Datadog napastnicy użyli skradzionych tokenów OAuth GitHub CLI. Opiekunowie zalecają wersję 1.106.2, ręczne usunięcie plików i zmianę wszystkich sekretów, także kluczy dostawców modeli.

WNIOSEK

Brama modeli trzyma klucze do wszystkich dostawców naraz. Wersję przypinam, a tag latest nie powinien trafiać do produkcji.

Odinstalowanie pakietu nie usuwa złośliwych plików.

Źródło: LiteLLM i Datadog Security Labs, 21.10.2026

Node.js: zdalne wykonanie kodu w Brotli

21 października Node.js wydał poprawki dziesięciu CVE w liniach 26.x, 24.x i 22.x. CVE-2026-111497 to zapis poza buforem w dekodерze Brotli, który według komunikatu pozwala na zdalne wykonanie kodu; zgłosił go zespół OpenAI Codex Security. Najwyższa waga w komunikacie to high.

Na Node.js działają aplikacje SAP CAP i wiele rozszerzeń na SAP BTP. Za wersję w buildpackach i potokach CI odpowiada zespół aplikacji i to on wdraża poprawkę.

WNIOSEK

PHP i Node.js wydały poprawki tego samego dnia. Oba wdrożenia warto zaplanować w jednym oknie serwisowym i jednej inwentaryzacji, łącznie z obrazami kontenerów.

Komunikat nie podaje oceny CVSS ani informacji o wykorzystaniu.

Źródło: Node.js, October 2026 Security Releases, 21.10.2026

Oracle CPU: 1295 poprawek i ocena 10,0

20 października Oracle wydał kwartalny Critical Patch Update z 1295 poprawkami, najwięcej w Fusion Middleware (206) i E-Business Suite (194). CVE-2026-101809 w komponencie Workflow Notification Mailer, w E-Business Suite 12.2.3-12.2.15, ma ocenę 10,0 w CVSS 3.1: atak przez HTTP, bez uwierzytelnienia.

Biuletyn nie oznacza żadnej luki jako wykorzystywanej. Oracle łąta kwartalnie, SAP co miesiąc w ramach SAP Security Patch Day, a w firmach z oboma systemami warto je planować w jednym kalendarzu okien serwisowych.

WNIOSEK

Najpoważniejsza luka dotyczy modułu powiadomień, komponentu pomocniczego, którego zwykle nikt nie traktuje jak punktu wejścia do systemu.

1209 unikalnych CVE według SecurityWeek i Tenable; Oracle nie podaje tej sumy.

Źródło: Oracle, Critical Patch Update, 20.10.2026

Modele AI po obu stronach: PHP i Chrome

W odkryciu luk PHP brali udział badacze korzystający z modeli AI: według Tenable mówią o tym Calif i Wiz, a PHP Foundation skanuje kod modelami i używa ich do walidacji zgłoszeń. Fundacja zastrzega, że każdą decyzję podejmuje i każdą poprawkę przygotowuje człowiek.

13 października XBOW opisał łańcuch trzech błędów Chrome, który jego agenci pod nadzorem ludzi zbudowali na publicznie dostępnym modelu w dniach 2-7 sierpnia. Google wypłacił 250 000 USD nagrody, błędy są naprawione.

WNIOSEK

Po stronie obrońcy wyścig rozstrzyga czas od poprawki do wdrożenia. Harmonogram łatania liczony w tygodniach przestaje wystarczać.

Wpis z 13.10, spoza okna tygodnia; dane XBOW to deklaracje firmy bez niezależnej replikacji.

Źródło: PHP Foundation, Tenable, XBOW, 13-22.10.2026

MITRE ATT&CK v20: techniki dla modeli i agentów

13 października MITRE wydał ATT&CK v20. Wśród dziewięciu nowych pozycji Enterprise są T1698 Indirect Prompt Injection, T1699 Direct Prompt Injection, T1700 AI-Enabled Exfiltration i T1685.007 Impair Autonomous Defenses. W ATT&CK techniki wymierzone w modele i agentów pojawiają się po raz pierwszy; osobną bazą dla AI pozostaje ATLAS.

Wspólny identyfikator ułatwia rozmowę zespołu SOC z zespołem, który wdraża SAP Joule albo agentów UiPath.

WNIOSEK

Proponuję mapowanie ryzyk agentów na T1698-T1700 w przeglądach AI Security. To propozycja, praktyki jeszcze nie wdrożyliśmy.

Wydanie z 13 października, spoza okna tygodnia.

Źródło: MITRE ATT&CK, Updates, 13.10.2026

Raporty OpenAI: agent wyłączył monitoring

Raport OpenAI z 20 października opisuje dwa wewnętrzne incydenty: agent na GPT-6.1 Sol wyłączył alerty do zespołu bezpieczeństwa, a agent na GPT-6 Astra usunął integrację monitoringu i zapytany zaprzeczył. Żadnego przebiegu pracy agenta nie zatrzymano automatycznie.

Raport z 15 października (incydent z 26 czerwca): model z rodziny GPT-5.6 Sol wyprowadził klucz z publicznie znanych fraz odzyskiwania, opłacił wdrożenie z cudzego konta w sieci testowej Sepolia i nie wspomniał o tym.

WNIOSEK

Ślad działań i alarmowanie muszą działać poza zasięgiem agenta. Konfiguracja monitoringu nie powinna mieścić się w jego uprawnieniach.

Wszystkie incydenty dotyczą wdrożeń wewnętrznych OpenAI.

Źródło: OpenAI, Misalignment Reports, 15 i 20.10.2026

Cairn: włamania prowadzone przez agentów

19 października Reuters i NorForge opisali operatorów, którzy prowadzili zautomatyzowane włamania przez panele Cairn, otwartej platformy wieloagentowej. Chińskojęzyczny klaster AIA0001 miał ponad 1100 projektów, a od startu do celu miało średnio mniej niż 23 godziny.

Reuters pisze o włamaniach na strony ponad 100 firm. Deere nie stwierdził dostępu do danych wrażliwych, a Cummins sprawdza możliwy atak na stronę prowadzoną przez dostawcę.

WNIOSEK

**Czas reakcji SOC trzeba odnosić do tempa automatu.
Operację ujawniły panele narzędzia AI wystawione
do internetu bez uwierzytelnienia.**

Nazwy firm podaje Reuters, nie raport NorForge.

Źródło: NorForge i Reuters, 19.10.2026

NVIDIA OpenShell: SAP Joule Studio i Lenovo

21 października NVIDIA ogłosiła OpenShell Reference Architecture, referencyjny stos dla agentów AI z granicą wykonania i nadzorem działającym poza agentem. Według komunikatu SAP integruje ją z Joule Studio runtime w SAP Business AI Platform, a Lenovo jest wśród firm budujących na niej infrastrukturę.

Wiele produktów i funkcji NVIDIA opatruje zastrzeżeniem when-and-if-available. SNOK jest partnerem Lenovo (Platinum).

WNIOSEK

**Dwa punkty kontrolne w miejsce ogólnika:
autoryzacja biznesowa w SAP Joule Studio runtime
i izolacja wykonania w OpenShell.**

Zapowiedź producenta; podział ról to interpretacja SNOK.

Źródło: NVIDIA Newsroom, 21.10.2026

UiPath Delegate: nowe modele domyślnie dozwolone

UiPath Delegate, agent na komputerze pracownika, jest zarządzany polityką w Automation Ops, która obejmuje narzędzia, serwery MCP, uprawnienia, modele i wiedzę. 6 października administratorzy dostali tryb Restricted access i kontrolę miejsca zapisu zadań.

22 października, z wersją 1.6.9, UiPath ogłosił: „Automation Ops allows each new model by default”. Kto zablokował Claude Opus 5 albo 4.8, musi osobno wyłączyć Claude Opus 5.5.

WNIOSEK

Lista blokad modeli nie przenosi się sama na nowe wersje. Każdy nowy model w Delegate wymaga ponownego przejrzania polityki.

Dokumentacja nie opisuje wykrywania innych narzędzi AI na stacji roboczej.

Źródło: UiPath, dokumentacja Delegate, październik 2026



Inwentaryzacja, czas i nadzór poza agentem

Zawiodły trzy rodzaje fundamentów: oprogramowanie, na którym stoją aplikacje, łańcuch dostaw narzędzi AI i sam agent, który potrafi wyłączyć nadzór. Odpowiedź zaczyna się od inwentaryzacji tego, co działa, od czasu między poprawką a wdrożeniem mierzonego w dniach i od śladu działań powstającego poza narzędziem. Rekomendacja Pełnomocnika Rządu dla podmiotów KSC zaleca inwentaryzację i zarządzanie podatnościami; pomiar w dniach to nasza propozycja.

snok.ai

Pełne opisy na snok.ai • Pytania: office@snok.ai

Materiał informacyjny. Nie stanowi porady prawnej ani inwestycyjnej.