Komentář ESET: Sociální síť Moltbook pro AI zpřístupnila data uživatelů

4.2.2026 - Lucie Mudráková, Vítězslav Pelc | ESET software

Společnost ESET komentuje aktuální případ zpřístupnění databáze sociální sítě Moltbook pro AI agenty.

Moltbook, rychle rostoucí sociální síť pro AI agenty, kvůli chybné konfiguraci omylem zpřístupnila celou svou databázi v Supabase. To umožnilo komukoli přistupovat ke všem datům platformy nebo je upravovat. Týkalo se to i 1,5 milionu API tokenů agentů, tisíců e-mailových adres uživatelů, soukromých zpráv (některé obsahovaly API klíče) a živých příspěvků.

Počet agentů na platformě byl navíc zavádějící – 1,5 milionu agentů ovládalo pouze asi 17 000 lidí. Problém vznikl kvůli tzv. „vibe codingu“, kdy zakladatel spoléhal na AI při vývoji platformy bez řádné bezpečnostní kontroly.

Incident zdůrazňuje bezpečnostní rizika u rychle vytvářených aplikací generovaných pomocí AI a potřebu bezpečných výchozích nastavení.

„Když jsou platformy poháněné umělou inteligencí vyvíjeny velmi rychle, základní prvky kybernetické bezpečnosti a ochrany soukromí bývají často tím prvním, na co se zapomene. A tento aktuální incident to nemohl ilustrovat výmluvněji. Skutečné riziko ale nepředstavují samotní AI agenti, nýbrž infrastruktura, která je za nimi. Tam mohou odhalené databáze a ledabylé ověřování totožnosti proměnit drobné přehlédnutí v závažné narušení bezpečnosti,” říká Vítězslav Pelc, mluvčí české pobočky společnosti ESET.

„AI služby vždy začínají se standardními či obecnými daty, ale jakmile se přiblíží citlivým oblastem, jako jsou finance nebo zdravotnictví, podobné případy budou jen podkopávat důvěru v technologie. Umělá inteligence může vývoj zrychlit a zlepšit, ale nikdy by neměla nahradit princip ‚security by design‘. Spustit službu rychle bez základních bezpečnostních opatření může být velmi drahá chyba,“ dodává Pelc.

Společnost ESET ve své predikci pro rok 2026 očekává, že AI agenti budou hluboce integrováni do podnikové infrastruktury, avšak jejich zabezpečení bude alarmujícím způsobem slabé. To dramaticky rozšíří útočnou plochu, jelikož i základní chyby v konfiguraci mohou způsobit právě vážné úniky dat. Rizika se skrývají i v samotných modelech a jejich možném zneužití.

Ekosystém veřejně dostupných AI modelů bude zažívat další boom, ale mnohé budou distribuovány s neznámou vnitřní logikou, což zvyšuje riziko útoků přes dodavatelský řetězec. V oblasti sociálního inženýrství pak pravděpodobně dojde k nárůstu vysoce kvalitních deepfakes a AI generovaných podvodů, které umožní i méně zdatným útočníkům provádět masivní kampaně. Velkou výzvou budou také pokročilí online boti, schopní ovlivňovat veřejné mínění, volby či automatizované náborové procesy.

Společnost ESET®, která byla založena v Evropě, je předním dodavatelem řešení kybernetické bezpečnosti s pobočkami po celém světě. Poskytuje špičková řešení kybernetické bezpečnosti, která pomáhají předcházet útokům ještě před jejich vznikem. ESET kombinuje technologie umělé inteligence (AI) a lidskou odbornost, čímž pomáhá předejít nově vznikajícím globálním kybernetickým hrozbám, ať již známým či dosud neznámým. Poskytuje zabezpečení pro firmy,

kritickou infrastrukturu a jednotlivce. Ať už jde o ochranu koncových zařízení, cloudu nebo mobilních zařízení, řešení a služby společnosti ESET, které využívají technologie umělé inteligence a kladou důraz na cloudové prostředí, zůstávají vysoce efektivní s minimálními nároky na uživatele.

Technologie ESET jsou vyvíjeny v EU a zahrnují robustní systém detekce a reakce, ultra-bezpečné šifrování a multifaktorovou autentizaci. S nepřetržitou obranou v reálném čase a silnou místní podporou udržuje ESET uživatele v bezpečí a firmy v chodu bez narušení jejich provozu. Neustále se vyvíjející digitální prostředí vyžaduje progresivní přístup k bezpečnosti. Jen v České republice nalezneme tři výzkumná a vývojová centra společnosti, a to v Praze, Jablonci nad Nisou a Brně. Výzkumné pobočky po celém světě podporují aktivity společnosti v rámci Threat Intelligence, stejně jako její silná globální síť partnerů.

Více informací o trendech v kyberbezpečnosti pro širokou veřejnost naleznete například v online magazínu Dvojklik.cz nebo v online magazínu o IT bezpečnosti pro firmy Digital Security Guide. Nejčastějším rizikům pro děti na internetu se věnuje iniciativa Safer Kids Online, která má za cíl pomoci nejen jejich rodičům, ale také například učitelům či vychovatelům zorientovat se v nástrahách digitálního světa.

Vysvětlení aktuálních kyberbezpečnostních pojmů a trendů najdete dále na stránkách Slovníku ESET, v podcastu RESET a na našich sociálních sítích Facebook, Instagram, LinkedIn a X.

Lucie Mudráková
Specialistka PR a komunikace
ESET software spol. s r.o.
tel: +420 702 206 705
lucie.mudrakova@eset.com

Vítězslav Pelc
Senior manažer PR a komunikace
ESET software spol. s r.o.
tel: +420 720 829 561
vitezslav.pelc@eset.com

https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/komentar-eset-socialni-sit-moltbook-pro-ai-zpristupnila-data-uzivatelu